

# REQUEST FOR PROPOSAL

## OSDC 2.0 -Extension of Odisha State Data Centre

Selection of System Integrator for Design, Build, Installation, Commissioning, Integration, and Operations & Maintenance of Non-IT & IT Infrastructure for Extension of Odisha State Data Centre.



**Tender Enquiry No: OCAC-NEGP-INFRA-008-2018-20038**

**Odisha Computer Application Centre (OCAC)**

(Technical Directorate of E&IT Department, Govt. of Odisha)

OCAC Building, Plot No.-N-1/7D, Acharya Vihar, RRL Post Office

This page has been kept left intentionally blank.

## Table of Contents

1.	Invitation for Bids .....	11
1.1.	Important Dates .....	11
1.2.	Bid Invitation .....	14
1.3.	Acronyms .....	17
2.	Project Objective & Brief Scope of Work .....	20
2.1.	About OCAC.....	20
2.2.	Project Objective .....	21
2.3.	Brief Scope of Work .....	23
	Scope of Work (Non IT) .....	24
	Scope of Work (IT) .....	26
	Operation and Facility Management .....	28
	Migration.....	28
3.	Pre –Qualification Criteria.....	29
3.1.	Pre-Qualification for Bidder.....	29
3.2.	Submission of the Proposal.....	33
3.3.	Deadline for Submission of Proposals.....	34
3.4.	Late proposals.....	34
3.5.	Proposal Prices.....	34
3.6.	Earnest money deposit.....	35
3.7.	Bid Validity Period.....	35
3.8.	Compliant /Completeness of response.....	36
3.9.	Pre-bid Meetings Clarification.....	36
3.10.	Responses to pre-bid queries and issue of corrigendum.....	37
3.11.	Amendment of Proposals .....	38
3.12.	Opening of proposals by OCAC.....	38
3.13.	Evaluation Procedure.....	38
3.14.	Technical Bid Evaluation Scoring Matrix .....	42
3.15.	Evaluation of Bids and Award of Contract. ....	52
3.16.	Deviations and Exclusions .....	54
3.17.	Rejection of Bids.....	54
3.18.	Notification of Acceptance of Proposal.....	54
4.	General Conditions of Contract .....	55
4.1.	Definition of Terms.....	55

4.2.	Total Responsibility .....	57
4.3.	Right to terminate the process.....	57
4.4.	Language of Proposal & Correspondence .....	57
4.5.	OCAC's Right to accept and to reject any or all proposals .....	58
4.6.	Modification and withdrawal of bids.....	58
4.7.	Contacting OCAC.....	58
4.8.	Knowledge of Site Conditions.....	58
4.9.	Failure to agree with terms & conditions of the contract.....	58
4.10.	Governing Law & Jurisdiction .....	59
4.11.	Termination and Effects of Termination.....	59
4.12.	Consequences of Breach and penalties.....	61
4.13.	Statutory Compliances.....	61
4.14.	Consequences of Termination.....	61
4.15.	Indemnification .....	62
4.16.	Limitation of Liability .....	63
4.17.	Dispute Resolution and Arbitration .....	64
4.18.	Force Majeure.....	65
4.19.	Confidentiality .....	65
4.20.	Fraud and Corrupt practices .....	66
4.21.	Exit Management Plan.....	68
4.22.	Severability and Waiver .....	71
4.23.	Applicability of Liquidated Damages.....	71
4.24.	Intellectual Property Rights .....	72
4.25.	Taxes and Duties.....	74
4.26.	Insurance .....	74
4.27.	Audit, Access and Reporting.....	75
4.28.	Ownership .....	75
4.29.	Safety Regulations.....	75
4.30.	Warranty of Equipment.....	76
4.31.	OEM Certificate of Equipment.....	77
4.32.	Comprehensive AMC of Equipment.....	78
4.33.	Spares and Performance of Equipment.....	78
4.34.	Change Order and Contract Amendment .....	78
5.	Design Consideration for OSDC 2.0 (Non-IT) .....	80

5.1.	Civil/ Non- IT Design Consideration .....	80
5.2.	Data Centre Build/Non IT Design Consideration.....	82
5.3.	Non IT Infrastructure (Scope of Work) .....	83
5.4.	Scope of Work – Electrical.....	94
5.5.	HT Power Distribution.....	96
5.6.	Diesel Generators .....	97
5.7.	MV Panels.....	98
5.8.	UPS Systems.....	99
5.9.	Cable, Bus Bar Trunks and Terminations .....	99
5.10.	Cable Schedule .....	100
5.11.	Cable/Conduit/Bus bar Laying .....	100
5.12.	Illumination .....	101
5.13.	Grounding/ Earthing .....	101
5.14.	Cable Pathways.....	102
5.15.	Scope of work – HVAC system .....	104
5.16.	Scope of Work – Safety, Security, Surveillance and Monitoring System.....	105
5.16.1	Addressable Fire Alarm System (AFAS).....	105
5.16.2	Aspiration Smoke Detection System or Very Early Smoke Detection System	106
5.16.3	Gas Based Fire Suppression System.....	106
5.16.4	Close Circuit Television System (CCTV).....	107
5.16.5	Access Control System .....	108
5.16.6	Water Leak Detection System.....	108
5.16.7	Rodent Repellent System (RRS) .....	109
5.16.8	Data Centre Infrastructure Management Tool.....	109
5.16.9	Visitor Management System.....	109
5.17.	Scope of Work -Network Passive Infrastructure, Racks, IPDU, etc. ....	110
5.18.	Upgradation of Utility equipment, integration and commissioning .....	111
5.19.	Tier Certification by Uptime Institute.....	111
5.20.	Data Centre Health Check Audit .....	111
5.21.	Indicative List of Equipment need to be considered for Buy Back option .....	113
5.22.	Technical, Functional and Operational requirements of Equipment’s (Non IT):	114
5.22.1	Uninterrupted Power supply (UPS) system with Battery back-up (For Critical Load).....	114
5.22.2	Uninterrupted Power supply (UPS) system with Battery back-up (For Non-Critical Load).....	117

5.22.3 Precision Air Conditioning System (Direct Expansion In-ROW) .....	119
5.22.4 Precision Air Conditioner (CRAC) for perimeter cooling of Power Rooms .....	123
5.22.5 Diesel Generator .....	125
5.22.6 Track Busway system (Continuous).....	127
5.22.7 Sandwich Type Bus duct System .....	129
5.22.8 MV Panels .....	131
5.22.9 Passive networking .....	135
5.22.10 DCIM .....	141
5.22.11 Asset Tracking.....	144
5.22.12 IT Rack.....	147
5.22.13 IPDU .....	149
5.22.14 Rack Access Control.....	151
5.22.15 33KV VCB Panels (HT Panel) .....	153
5.22.16 Dry Type Transformers.....	155
5.22.17 Fire Detection & Alarm System .....	161
5.22.18 Gas Based Fire Suppression System: - Suppression system (NOVEC 1230).....	162
5.22.19 Access Control System .....	166
5.22.20 High Sensitivity Smoke Detection System.....	168
5.22.22 IP Based CCTV System .....	174
5.22.23 Water Leakage Detection System .....	176
5.22.24 Ultrasonic Rodent Repellent system.....	177
5.22.25 Physical Access Control System .....	179
5.22.26 3D X-ray Baggage Scanner.....	183
6. Detailed Scope of Work.....	187
6.1. Tier Certification by Uptime Institute.....	187
6.2. IT System Design Consideration.....	188
6.2.1 SITC of IT Infrastructure: .....	188
6.3. Key considerations for designing the Odisha State Data Centre 2.0:.....	189
I. Scalability .....	189
II. High Availability .....	190
III. Interoperability .....	190
IV. Manageability .....	190
V. Cyber Security .....	190
VI. Integration of OSDC with SWAN.....	190
VII. IPv6 Readiness .....	191

VIII.	Cloud Services Provisioning .....	191
6.4.	Inter -Intra Rack Connectivity .....	191
6.5.	Indicative Logical Schematic .....	191
6.5.1	High Level Indicative Logical Diagram for OSDC 2.0 .....	192
6.6.	IT Infrastructure (Scope of Work).....	196
6.6.1	Detailed Functional Scope of Work .....	196
6.6.2	Design Validation and Change .....	204
6.6.3	Installation and Configuration of the Commissioned IT Infrastructure .....	204
6.6.4	Deployment Phase .....	204
6.6.5	Procurement & Delivery of IT infrastructure components.....	205
6.6.6	Implementation .....	206
6.6.7	Migration to OSDC 2.0.....	206
6.7.	Operations & Maintenance.....	207
6.7.1	Onsite Support .....	207
6.7.2	Technical Support .....	208
6.7.3	System Maintenance and Management .....	208
6.7.4	System Administration.....	209
6.7.5	Storage Administration .....	210
6.7.6	Database Administration .....	211
6.7.7	Backup / Restore .....	211
6.7.8	Network Monitoring .....	211
6.7.9	Firewall Monitoring and Management.....	213
6.7.10	Network Based Intrusion Prevention System - Monitoring and Management .....	213
6.7.11	Patch Management.....	214
6.7.12	Monitoring & Management.....	214
6.7.13	Other Support Services.....	215
6.8.	Health Safety Environment.....	216
7.	Minimum Technical Specification – IT .....	219
7.1.	Server Type A & B – Rack Server.....	219
7.2.	Core Router .....	221
7.3.	Spine Switch .....	224
7.4.	Leaf Switch (Fibre) .....	226
7.5.	Leaf Switch (Copper).....	228
7.6.	Management Switch -1.....	231
7.7.	Management Switch -2.....	232
7.8.	San Switch (128 Ports).....	234

7.9.	San Switch (48 Ports) .....	235
7.10.	Enterprise Storage.....	236
7.11.	Tape Library .....	239
7.12.	Link Load Balancer .....	240
7.13.	Next Generation Firewall.....	241
7.14.	AAA.....	245
7.15.	DDOS .....	247
7.16.	Endpoint Security.....	248
7.17.	Server Security Solution .....	252
7.18.	Vulnerability Assessment Solution .....	253
7.19.	Cloud Management & Orchestration Solution.....	255
7.20.	Virtualization Software.....	257
7.21.	Openstack Cloud Framework.....	258
7.22.	Platform as a Service.....	261
7.23.	Enterprise Management System .....	263
7.24.	SDN Controller .....	269
7.25.	Anti- APT Solution.....	271
7.26.	DLP Solution.....	273
7.27.	Laptop.....	276
7.28.	Desktop.....	278
7.29.	Multi-Function Printer (Print, Copy, Fax, Scan) .....	279
7.30.	KVM Switch (IP Based).....	280
7.31.	Data Centre Access Management.....	282
8.	Project Timelines and Liquidated Damages .....	284
8.1	Liquidated Damages Table .....	288
9.	Payment Schedule.....	290
10.	Service Level Agreement.....	293
10.1	Brief Description of the Services to be provided .....	293
10.2	SLA Definitions.....	293
10.3	Category of SLA.....	294
10.4	Targets of Service Level Agreement.....	294
10.5	Performance Related Service Levels .....	295
10.6	IT Infrastructure Service Level.....	297
10.7	Virtual Infrastructure related Service Levels .....	300



10.8	Security and Incident Management Service Levels.....	301
10.9	Help Desk Support Services Level.....	302
10.10	Manpower Service Levels.....	305
10.11	Compliance & Reporting Procedures .....	307
10.12	Civil and Electrical Major and Minor Works.....	309
10.13	SLA for existing Data Centre .....	310
10.14	Important Note .....	312
10.15	SLA Change Control .....	313
10.16	SLA Change Process .....	313
10.17	Penalty .....	314
11.	Project Management.....	315
11.1	Partial Acceptance Test (PAT).....	315
11.2	Final Acceptance Testing (FAT) .....	316
11.3	Roles and Responsibilities.....	316
11.4	Training.....	318
12	Minimum Bill of Quantity .....	320
12.1	Bill of Quantity – Non- IT OSDC 2.0.....	320
12.2	BOQ of IT items.....	327
13	Operations and Maintenance Management.....	329
13.1	Commissioning of System .....	329
13.2	Human Resource and Planning.....	331
13.3	Policies and Procedures .....	334
13.4	Maintenance Management.....	335
13.5	Operations & Maintenance Monitoring .....	336
13.6	Access Management .....	336
13.7	Training and Development .....	337
13.8	Documentation.....	337
13.9	Reporting.....	338
13.10	Monthly reports.....	339
13.8.2	Quarterly reports .....	339
13.8.3	Half-Yearly reports .....	340
13.8.4	MIS reports and deliverables .....	340
13.8.5	Incident Reporting.....	340
13.8.6	Performance - Monitoring, Management and Reporting .....	342
13.8.7	Constitution of the Team .....	342

13.8.9 O & M Roles and Responsibilities .....	344
13.8.10 Certification .....	344
13.8.11 Automation of Services .....	345
13.11 Handing Over Taking over (HOTO Plan) .....	345
14 Proforma and Schedules .....	348
14.1 Proforma 1: Proposal Covering Letter .....	348
14.2 Proforma 2: Declaration of Acceptance of Terms & Conditions of RFP.....	350
14.3 Proforma 3: Undertaking on Total Responsibility.....	351
14.4 Proforma 4: Format of Technical Proposal Document.....	352
14.5 Proforma 5: Forwarding Letter for Earnest Money Deposit.....	353
14.6 Proforma 6: Format for furnishing Earnest Money Deposit.....	355
14.7 Proforma 7: Company Profile of Bidder .....	356
14.8 Proforma 8: Declaration regarding Clean Track Record .....	357
14.9 Proforma 9: Undertaking on litigation .....	358
14.10 Proforma 10: Undertaking on Not Being Black-Listed.....	359
14.11 Proforma 11: Undertaking of Service Level Compliance .....	360
14.12 Proforma 12: Authorization Letters from all OEMs.....	361
14.13 Proforma 13: OEM’s Support Form.....	362
14.14 Proforma 14: Warranty Certificate.....	364
14.15 Proforma 15: Technical specification compliance by OEM/Bidder. ....	365
14.16 Proforma 16: Statement of No Deviation from Requirement Specifications .....	366
14.17 Proforma 17: Bidder’s Annual Turnover.....	367
14.18 Proforma 18: Bidder’s Net worth.....	368
14.19 Proforma 19: Project Credentials Format.....	369
14.20 Proforma 21: Format for providing CV of Key Personnel.....	370
14.21 Proforma 22: Detailed Timelines and Work Plan with proposed Manpower Strength.....	371
14.22 Proforma 23: Format for Unpriced Bill of Material.....	374
14.23 Proforma 24: Format for Performance for Bank Guarantee (PBG) .....	375
14.24 Proforma 25: Format of Commercial Proposal Document .....	377
14.25 Proforma 26: Undertaking on Exit Management and Transition .....	379
<b>Annexure -A (As-Is Inventory List of Current SDC ) .....</b>	<b>380</b>
Server Detail.....	380
Network Equipment.....	384
Storage Equipment Details.....	386

Current Desktop, Laptop & Printer details ..... 387

## 1. Invitation for Bids

### 1.1. Important Dates

Sl. No.	Activity	Timeline
1.	Release of RFP	09/10/2020
2	Site Survey by bidders	13/10/2020 and 14/10/2020
3.	Last date of receipt of pre-bid queries online	16/10/2020 by 5 PM
4.	Pre-bid Meeting date	21/10/2020 at 11:30 AM
5.	Posting of response to queries and release of corrigendum, if any	29/10/ 2020
6.	Last date for submission of Bids hard copy of documents – 1 Original and 1 CD/DVD	21/11/ 2020 by 3:00 PM
6.	Date of opening of pre-qualification bids	21/11/ 2020 at 4:30 PM
7.	Date of opening of Technical Bids	To be notified later
8.	Date of opening of Commercial Bids	To be notified later

## Disclaimer

The information contained in this RFP or subsequently provided to bidders, whether verbally or in documentary or any other form by or on behalf of OCAC or any of its employees or advisers, is provided to bidders on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is issued by OCAC. This RFP is not an agreement and is neither an offer nor invitation by OCAC to the prospective bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in the formulation of their bid pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by OCAC in relation to extension of OSDC. Such assumptions, assessments and statements do not purport to contain all the information that each applicant may require.

This RFP may not be appropriate for all persons, and it is not possible for OCAC, its employees or advisers to consider the objectives, technical expertise and particular needs of each party who reads or uses this RFP.

The assumptions, assessments, statements and information contained in this RFP, may not be complete or adequate. Each bidder should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments and information contained in this RFP and obtains independent advice from appropriate sources. Information provided in this RFP to the bidders is on a wide range of matters, some of which depends upon interpretation of law.

OCAC, makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this Tender or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the Tender and any assessment, assumption, statement or information contained therein or deemed to form part of this Tender or arising in any way in this Bid Stage.

OCAC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever, caused arising from reliance of any Bidder upon the statements contained in this Tender. OCAC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this Tender. The issue of this Tender does not imply that OCAC is bound to select a Bidder or to appoint the Preferred Bidder,

as the case may be, for the Project and OCAC reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

OCAC reserves all the rights to cancel, terminate, change or modify this selection process and/or requirements of bidding stated in the RFP, at any time without assigning any reason or providing any notice and without accepting any liability for the same.

The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. OCAC accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on the law expressed herein. OCAC its employees and advisers make no representation or warranty and shall have no liability to any person including any applicant under any law, statute, and rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this selection process.

OCAC also accepts no liability of any nature whether resulting from negligence or otherwise however, caused arising from reliance of any bidder upon the statements contained in this RFP.

The bidder shall bear all its costs associated with or relating to the preparation and submission of its Proposal including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by OCAC or any other costs incurred in connection with or relating to its proposal. All such costs and expenses will remain with the bidder and OCAC shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a bidder in preparation or submission of the bid proposal, regardless of the conduct or outcome of the selection process.

### General Instructions to Bidders

- While every effort has been made to provide comprehensive and accurate background information, requirements, and specifications, Bidders must form their own conclusions about the requirements. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.
- All information to be supplied by Bidders will be treated as contractually binding on the Bidders, on successful award of the assignment by OCAC on the basis of this RFP.

- No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of OCAC with the bidder. OCAC may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of OCAC.
- This RFP supersedes and replaces any previous public documentation & communications in this regard and bidders should place no reliance on such communications.

## 1.2. Bid Invitation

Odisha Computer Application Centre invites offer/proposal from interested bidders for “Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar” for a period of five (5) years from date of acceptance of work order. This RFP document is being published on web Portal “<https://www.ocac.in>”, this section provides general information about the issuer, important dates, and addresses for bid submission & correspondence for the bidders.

The bidders are advised to study the RFP document carefully. Submission of bids shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

Odisha Computer Application Centre is the nodal agency of Odisha State working towards promotion & implementation of IT and e-Governance. It is the single-point of access to any IT business opportunity in Odisha and encourages various players in the field of IT to come forward and invest in the State of Odisha. OCAC is committed to generate IT business for the public/private sector with a mandate from the Government to develop IT in the state. This includes opportunities for software development, supply of hardware & peripherals, networking and connectivity, web applications, e-commerce, IT training and an entire gamut of direct and indirect IT businesses.

The Bid document may be purchase by any interested Bidder on submission of a written application along with the Bid document fee of Rs. 25,000/- in the form of Demand Draft from a scheduled bank in India in favour of Odisha Computer Application Centre, payable at Bhubaneswar, during office hours on any working day. The complete bid document has also been published on the website [www.ocac.in](http://www.ocac.in), [www.odisha.gov.in](http://www.odisha.gov.in), for downloading. The downloaded bid document shall also be considered valid for participation in the bid process but such bid documents should be submitted along with the required Bid document fee as mentioned.

**Fact Sheet**

Proposal inviting agency	<b>Odisha Computer Application Centre</b>
Start date of Uploading document	09/10/2020
Non Refundable RFP Cost	Rs. 25,000/- (Twenty Five Thousand only) exclusive of 18% GST in the form of DD/ Bankers Cheque in favour of "OCAC" payable at Bhubaneswar from a nationalized / scheduled commercial bank in India.
Sale of RFP Document	From 09/10/2020 to 08/11/2020, till 11.00 AM Also download from our website <a href="http://www.ocac.in">www.ocac.in</a> ,
The contact information	<a href="#">General Manager (Admin)</a> Odisha Computer Application Centre, N1/ 7D, Acharya Vihar Square, Near Planetarium, P.O. – RRL, Bhubaneswar 751013 Ph. - 0674-2582850/ 2588064 Website: <a href="http://www.ocac.in">www.ocac.in</a>
Last date and time for submission of proposal	21/11/2020 by 3:00 PM
Earnest Money Deposit - (EMD)	Rs.2,00,00,000/- (Two Crore only) in form of Bank Guarantee in the prescribed format in favour of "OCAC" payable at Bhubaneswar from a nationalized / scheduled commercial bank in India.
Pre bid Conference	On 21/10/2020 at 11:30 AM (Bidders queries should reach as on before 19/10/2020 05:00 PM - Last date for receiving queries through E-mail: <a href="mailto:osdc@ocac.in">osdc@ocac.in</a> & <a href="mailto:sk.bhol@nic.in">sk.bhol@nic.in</a> )
Posting of response to queries and release of corrigendum, if any	29/10/2020
Opening of Pre-Qualification Bid	21/11/2020 by 04:30 PM
Opening of General cum Technical Presentation by the qualified bidder.	Will be intimated later
Opening of Commercial Bids	Will be intimated later
Bid validity	Bid must remain valid up to 180 (One Hundred & Eighty) days from the actual date of submission of bid.
Address for Correspondence and Clarifications	<b>General Manager, OCAC, Odisha Computer Application Centre, N1/ 7D, Acharya Vihar Square, Near Planetarium, P.O. – RRL, Bhubaneswar 751013 Ph. - 0674-2582850/ 2588064 Website: <a href="http://www.ocac.in">www.ocac.in</a></b>



	<b>Mr. S.K. Bhol</b> <b>Senior Technical Director NIC,</b> <b>&amp; Project Manager, OSDC</b> <a href="mailto:osdc@ocac.in">osdc@ocac.in</a> & <a href="mailto:sk.bhol@nic.in">sk.bhol@nic.in</a>
Language of the proposal	This proposal should be filled in English language only. If any supporting documents are to be submitted, in any other language other than English, then translation of the same in English language, attested by the Bidder should be attached.
Proposal currency	Bidder shall be quote prices in Indian Rupees (INR) and will receive payment is Indian Rupees only

Please visit web site "<http://www.ocac.in>" for complete detail.

The Bidders are advised to submit the bids well in advance of the deadline as OCAC/GoO will not be liable or responsible for non-submission of the bids because of any problems whatsoever.

### 1.3. Acronyms

List of acronym that has been used in this document has mentioned here along with its full form/meaning.

S NO	Abbreviations	Description/ Definitions
1.	<b>OCAC</b>	Odisha Computer Application Centre
2.	<b>OSDC</b>	Odisha State Data Centre
3.	<b>OSDC 2.0</b>	Odisha State Data Centre 2.0
4.	<b>BOM</b>	Bill of Material
5.	<b>BOQ</b>	Bill of Quantity
6.	<b>BTA</b>	Business Transaction Activity
7.	<b>CAPEX</b>	Capital Expenditure
8.	<b>Cr.</b>	Crores
9.	<b>CCTV</b>	Closed Circuit Television
10.	<b>DaaS</b>	Database as a Service
11.	<b>DC</b>	Data Centre
12.	<b>DG</b>	Diesel Generator
13.	<b>DOT</b>	Department of Telecom
14.	<b>DPR</b>	Detailed Project Report
15.	<b>EMS</b>	Enterprise Management System
16.	<b>FAT</b>	Final Acceptance Test
17.	<b>FTP</b>	File Transfer Protocol
18.	<b>G2B</b>	Government to Business
19.	<b>G2C</b>	Government to Citizens
20.	<b>G2G</b>	Government to Government
21.	<b>HLD</b>	High Level Design
22.	<b>HPC</b>	High Performance Computing
23.	<b>HVAC</b>	Heating, Ventilation, and Air Conditioning
24.	<b>HT</b>	High Tension
25.	<b>IaaS</b>	Infrastructure as a Service
26.	<b>IP</b>	Internet Protocol
27.	<b>IPS</b>	Intrusion Prevention System
28.	<b>IBMS</b>	Integrated Building Management Systems
29.	<b>ISO</b>	International Organization for Standardization
30.	<b>ISP</b>	Internet Service Provider
31.	<b>IT</b>	Information Technology

S NO	Abbreviations	Description/ Definitions
32.	<b>IOT</b>	Internet over Things
33.	<b>ITSM</b>	IT Service Management
34.	<b>LAN</b>	Local Area Network
35.	<b>LT</b>	Low Tension
36.	<b>MeitY</b>	Ministry of Electronics and Information Technology
37.	<b>MPLS</b>	Multiprotocol Label Switching
38.	<b>NFPA</b>	National Fire Protection Agency
39.	<b>NGFW</b>	Next Generation Firewall
40.	<b>NMS</b>	Network Management Server
41.	<b>NOC</b>	Network Operations Centre
42.	<b>O&amp;M</b>	Operations and Maintenance
43.	<b>OEM</b>	Original Equipment Manufacturer
44.	<b>OPEX</b>	Operational Expenditure
45.	<b>PAC</b>	Precision Air Conditioning
46.	<b>PAHU</b>	Precision Air Handling Unit
47.	<b>PaaS</b>	Platform as a Service
48.	<b>POE</b>	Power over Ethernet
49.	<b>POI</b>	Point of Interconnect
50.	<b>PDU</b>	Power Distribution Unit
51.	<b>PUE</b>	Power Usage Effectiveness
52.	<b>QOS</b>	Quality of Services
53.	<b>SAN</b>	Storage Area Network
54.	<b>SaaS</b>	Software as a Service
55.	<b>SDC</b>	State Data Centre
56.	<b>SDN</b>	Software Define Network
57.	<b>SIEM</b>	Security Information and Event Management
58.	<b>SWAN</b>	State Wide Area Network
59.	<b>STP</b>	Spanning Tree Protocol
60.	<b>TCP</b>	Transmission Control Protocol
61.	<b>TCV</b>	Total Contract Value
62.	<b>GoO</b>	Government Of Odisha
63.	<b>UPS</b>	Uninterrupted Power Supply
64.	<b>VRF</b>	Virtual Routing & Forwarding
65.	<b>VESDA</b>	Very Early Smoke Detection Apparatus
66.	<b>WAN</b>	Wide Area Network

S NO	Abbreviations	Description/ Definitions
67.	<b>WLD</b>	Water Leak Detection System

## 2. Project Objective & Brief Scope of Work

### 2.1. About OCAC

Odisha Computer Application Centre (OCAC) alias OCAC is the Designated Technical Directorate of Electronics & Information Technology Department, Government of Odisha, has evolved through years as a Centre of excellence working towards promotion & implementation of IT solutions and e-Governance. It is the single-point of access to any IT business opportunity in Odisha and encourages various players in the field of IT to come forward and invest in the State of Odisha.

Odisha Computer Application Centre (OCAC) is engaged in businesses related to Electronics, Computer goods and IT services. The directorate caters to the technological needs of the government and carries out IT project conceptualization and implementation for the State Government Departments and agencies.

OCAC is committed to generate IT business for the public/private sector with a mandate from the Government to develop IT in the state. This includes opportunities for software development, supply of hardware & peripherals, networking and connectivity, web applications, e-commerce, IT training and an entire gamut of direct and indirect IT businesses.

Odisha Computer Application Centre, the Designated Technical Directorate of Information Technology Department, has contributed significantly to the steady growth of IT in the State and deliver value to the beneficiaries by delivering superior value through its services and solutions. So it helps IT to reach the common citizen so as to narrow down the Digital Divide and widespread applications of IT is establishing a system where the citizens are receiving good governance ensuring speed of decisions from a transparent Government through an effective e-Governance System.

- To Provide excellent electronic, IT Goods, IT Services to the Government of Odisha.
- To create a robust IT eco-system for enhancing competitiveness and productivity of the key economic sectors affecting the lives of the majority of the population of the State.
- To disseminate IT and ITeS activities across the state so that rural population is equally benefited.
- To provide seamless and reliable citizen-centric services and information for the public, thereby enhancing efficiency, transparency and accountability of Government.
- To help its customers adapt themselves to the modern management techniques.

## 2.2. Project Objective

The State Data Centre (SDC) is a key-supporting pillar of e-Government initiatives for delivering services to the citizens with greater reliability, availability and serviceability. SDC provides better operations & management control and minimizes overall cost of Data Management, IT Management, Deployment and other costs.

State Data Centres are one of the three infrastructure pillars structured by the National eGovernance Plan (NeGP) to facilitate web-enabled anytime, anywhere access. State Data Centres are conceptualized with the objective of providing a common enabling infrastructure to the States to cater to their e-governance applications hosting requirements of the entire state government and its departments. It was live in October, 2011 to host services, applications and infrastructure and to provide efficient electronic delivery of G2G, G2B and G2C services.

Ministry of Information Technology and Electronics (MeitY), Government of Odisha (GoO) were the key and core stakeholder of implementation of various Mission Mode Projects under NeGP. A Composite Team has been formed with the officers from OCAC and National Informatics Centre (NIC) for shouldering the responsibility of techno-administrative support of overall SDC operations, management and hosting various departmental applications at SDC.

To extend the success of computerization, Government of Odisha (GoO) in support with its nodal agency had set up SDC for hosting the departmental applications. Presently, the Data Centre is catering the IT infrastructural needs of all departmental owned applications and e-Governance applications envisaged to provide a wider range of services to the Citizens of Odisha by computerizing the operations of various department of GoO.

The existing State Data Centre (SDC) is a core infrastructure project at OCAC building, over an area of 4000 Sq. ft. (approx.) built in the year 2011, which included the server farm area of 1500 Sq. ft. (approx.) to facilitate on-premises hosting of Government applications. More than 165 applications have already been hosted under virtualized/cloud environment (Hyper-V/ VCloud suite) in the SDC. Separate remote Data Recovery services have been provisioned at National Data Centre, Shastri Park, New Delhi through storage based replication of data. Envisaged future BCP/ Disaster Recovery (DR) for Applications hosted with SDC shall be provisioned at an alternate site.

OCAC offers expansion /extension of SDC in the form of the Tier III standard State Data Centre in first floor of OCAC Towers which will be built exclusively and dedicatedly for extension of Odisha State Data Centre (OSDC 2.0) within the same campus. Since, the State Data Centre has already

completed more than eight (9) years of operation, most of the compute, storage and network is utilized and would require upgradation.

The technology used in the current Data Centre is Ten years old and would require refresh to keep up to date for security reasons and as per industry standards. For the purpose of design, supply, installation, configuration, integration, operation & maintenance of Civil, IT and Non IT infrastructure of the proposed Tier-III OSDC 2.0, proposals are invited from the perspective bidders through this RFP. Currently, most of the items of the existing SDC are in a state of extended support by the respective Original Equipment Manufacturers (OEM). In view of the above, immediate replacement of the devices which are in extended support is extremely important for smooth operation of OSDC. The Data Centre is currently facing a huge demand from the State user departments for hosting their applications.

Odisha State Data Centre 2.0 will facilitate to host applications of various user departments of State as well as PSU's on a common infrastructure leading to ease of integration and efficient management, ensuring that computing resources and the support connectivity infrastructure (SWAN) is adequately and optimally used. The OSDC 2.0 will be equipped to host / co-locate systems (e.g. Cloud, Web Servers, Application Servers, Database Servers, SAN and NAS etc.) applications using the centralized computing power. The IT infrastructure will ensure host multiple applications with high availability, scalability, reliability, portability, and centralized authenticating system to authenticate the users to access their respective systems.

### 2.3. Brief Scope of Work

The extension of Odisha State Data Centre will provide a hosting space to meet the demand of the user departments for hosting their applications in the State Data Centre. Also, to create a highly secure flexible, automated , managed cloud service environment deploying the latest industry computing infrastructure for keeping the user department applications secure , highly scalable and available.

There is a need to set up strategic infrastructure that facilitates high availability, quick scalability, efficient management & optimized utilization of resources. To fulfil this requirement, OCAC intends to set up a Tier-III data Centre OSDC 2.0 with high availability to facilitate the government offices to access to servers, storage, databases, and a broad set of application services over the Internet. It will provide better operations and management control and minimize overall cost of Data Management, IT Management, Deployment and other costs.

OSDC 2.0 intends to unify the virtual and physical infrastructure with cloud and legacy systems along with underlying infrastructure capability to support containers, bare metal, and virtualized workloads while treating compute, storage, and network devices as flexible pools of resources. It is envisaged that everything should work together seamlessly, as opposed to fragmented silos and any particular technology should fit together into the overall, cohesive picture while being a good fit for every use case and workload – be it the requirement of OCAC & E & IT Department itself or the requirement of any user line department of the State.

OCAC should be able to compose and then recompose these flexible resources with automation depending on the individual workload requirements or the application needs. As all workloads are not created equal, proposed OSDC 2.0 should offer flexibility to support this workload elasticity and agility such as it will allow applications that need large amounts of storage, while allowing other applications that need a lot of network bandwidth or relatively higher compute performance. Capacity planning and their scalability needs should be the key consideration factors while doing the systems engineering of OSDC 2.0 in totality.

Target intention is that the OSDC 2.0 should be more conducive to infrastructure fluctuations and more programmable while enabling the underlying infrastructure to support containers, bare metal, and virtualized workloads. Moreover, the planned OSDC 2.0 transformation needs to be ready for both composable as well as hyper-converged workloads from present day so that hyper-converged solutions can be added incrementally as needs arise in future and as the hyper-converged



technology goes on to support more types of workloads beyond today's support of only virtualized workloads.

The minimum specified scope of work to be undertaken by the bidder for Design, Supply, Installation, Testing, Commissioning, Integration & Operations and Maintenance of the proposed OSDC 2.0 at Bhubaneswar as per the scope mentioned below. The selected bidder shall ensure an uptime more than 99.982% (Tier III) guideline on a quarterly basis for period of five years after Go-Live of the Project.

This section describes the scope of work (SOW) of the System Integrator (SI) for creation of Odisha State Data Centre – OSDC 2.0. This SOW is not limited to the following as described but includes all the possible scopes that may be required for execution of the project based on standards and best practices. In case, any bidder feels that any requirement that is not explicitly mentioned here but is essential to complete this project may, bring to the notice of the authority during pre-bid meeting

The minimum specified work to be undertaken by the bidder for setting up and operating the proposed OSDC 2.0 has been categorized as under:

- Schedule I: Supply, Installation, Testing and Commissioning of the Non-IT Infrastructure of the proposed OSDC 2.0 at OCAC Towers, Bhubaneswar.
- Schedule II: Supply, Installation, Testing and Commissioning of the IT Infrastructure of the proposed OSDC 2.0 at OCAC Towers, Bhubaneswar.
- Schedule III: Migration of existing applications and integration of existing DC.
- Schedule IV: Acceptance Tests (PAT and FAT), Uptime Certifications.
- Schedule V: Operations and Maintenance services for the complete Infrastructure at OSDC 2.0 at OCAC Towers, Bhubaneswar for the period of 5 years from the date of successful acceptance by OCAC.

*Note: The bidders are requested to submit their proposals for these phases/Schedules in the same bid which would be combined for evaluation purposes.*

### Scope of Work (Non IT)

#### Data Centre Non-IT physical Infrastructure

##### i. Civil & Interior Works

- Raised flooring inside server hall, Vitrified/Marble tile flooring, tile carpet flooring in support area, PCC flooring on all area.
- Modular false ceiling in support area

- Fire rated glass partition in server hall, toughened glass partition, gypsum partition in support area.
  - Fire rated doors, glass doors and flush doors, Shutters, Grills
  - POP and paint
  - Furniture and accessories, Ramps, rolling shutters, grill partition and doors.
  - Toilet interiors with faucets, fitting, wall and floor tiles plumbing and all scope to make the work complete.
  - Brick wall as required at different area
- ii. HT and MV Power and distribution
- Replacement of HT and metering panel, cables , transformer, BBT and transformer output panels
  - Main and sub LT panels. `
  - Distribution panels and DBs
  - Lighting and wiring
  - Earthing and Grounding
  - Replacement of Diesel generators, exhaust stack, HSD tank, Fuel pump etc.
  - Track Busway ( BBT) inside server hall
  - Intelligent PDUs
  - Modular UPS systems with lithium ion batteries for IT load, Non critical UPS with VRLA batteries.
  - All cabling, raceways, cable trays, tagging, connectors, terminations
- iii. Precision and Comfort Air conditioning
- Removal of AHU and closing the pipes
  - In-row cooling for high and low/medium density racks
  - Perimeter cooling for power room
  - ODU platform
  - Floor and ceiling insulation
  - VRV / VRF comfort cooling for support area with cassette indoor units
  - Precision cooling for UPS and Power room
  - All cabling, Piping, Containment, Floor grills, indoor units for support area etc.
- iv. Safety, Security, Surveillance and Monitoring
- Addressable fire alarm system for server hall, support area utility building.
  - Removal for fire hydrant piping from server hall area.
  - Aspiration smoke detection system in server hall
  - Gas based suppression system in server hall, UPS and Power room

- Close circuit television system
  - Access control system, visitor management system, flap barriers, baggage scanners, metal detectors, full height turnstiles etc.
  - Water leak detection system
  - Rodent repellent system
  - Data Centre infrastructure monitoring system
- v. Network passive infrastructure
- Server and Network racks
  - Copper and fiber structure cabling
  - Asset tracking and rack access control system
  - Fiber and copper pathways.

### Scope of Work (IT)

The overall Scope of Work (SoW) for the bidder to be appointed through this RFP for the IT infrastructure includes the following but not limited to:

- Supply, installation and configuration, testing and commissioning of compute infrastructure (hardware & software) such as Servers, Operating Systems and cloud orchestration, virtualization, management etc.
- Supply, installation, configuration, testing and commissioning of Network infrastructure like, Router, Core switch, Leaf switch and management switch, Link Load balancer & SDN controller, including laying of inter-rack and intra-rack structured cabling (OFC and Copper)
- Supply, installation, configuration, testing and commissioning of Storage Area Network with Storage system, SAN switches, Tape Library, backup and restore, including laying of FC cables.
- Supply, installation, configuration, testing and commissioning of Security infrastructure like D-DOS, Next Generation Firewalls, VA solution, Anti-APT solution, DLP solution etc.
- Centralized cloud environment to host multiple applications with simplified operations and increased application responsiveness to support next generation of distributed applications. The solution should be able to provide a unified management of performance, capacity and compliance of cloud infrastructure along with on premise Service implementation for Orchestration layer.
- Supply, installation, configuration, testing and commissioning of Antivirus, HIPS, On Prem VM based solutions and Enterprise Management System.
- **Desirable capabilities of Software Defined Cloud Enabled Data-Centre –**

- Software defined compute, software defined storage, software defined network and software defined security
- Unified life cycle management for the overall cloud solution with enterprise class support.
- Future proof to adopt technology changes and innovation.
- Open Standards and Open Source based private cloud landscape
- Should have a capability to manage cross platform virtualization with cloud management platform.
- OpenStack/Open Source based framework for the cloud deployment
- Complete agent-less automation with life cycle management.
- Single and Unified run-time environment.
- The solution should be able to scale to IaaS, PaaS and SaaS & DaaS if desired.
- It should have capability to manage hybrid cloud environment.
- It should support generic x86 environment and leading hardware OEM
- Data Driven & Ready for the unpredictable
- Ready for DevOps & Application Lifecycle Management
- Five years on-site comprehensive maintenance and provisioning of services of all the ICT Infrastructure and all its components should be supplied with a provision of onsite spares on 24x7x365 basis after successful execution and acceptance by OCAC.
- Onsite support for Data Centre Operations on 24 x 7 x 365 basis by qualified and trained engineers/professionals for a period of five years to ensure more than 99.982% service availability.
- Bidder to get following Data Centre Certification within 6 months from Go-Live and all related cost for the certification will be borne by bidder :
  - ISO 9001
  - ISO 27001
  - ISO 20000
  - ISO 27017
  - Uptime Tier III certification for Design, Construction and Operation
- Cost of sustenance audit for above certification shall be responsibility of the bidder for the entire contract period.
- All application (including Application Data) needs to be migrated from SDC to OSDC 2.0.
- Existing Internet connectivity will be relocated from SDC to OSDC 2.0, successful bidder will manage the internet connectivity with respective ISPs.
- Network and security devices need to be consolidated as well as integrated from SDC to OSDC 2.0

## Operation and Facility Management

- Annual Maintenance of Products
- DC office Maintenance
- Service Level Adherence
- Resource Deployment
- Standard Operating Procedures (SOP)
- Periodic Health Audit of NON-IT infrastructure

## Migration

- Hardware, Application and Database Migration from existing SDC to OSDC 2.0 is an essential part of the project.

### 3. Pre –Qualification Criteria

The bidder should have mandatory pre-qualification as per the following table. The proposal of the bidder who is fulfilling the mandatory pre-qualification criteria shall be consider for technical evaluation. The proposal would liable to be rejected if any bidder does not fulfil any pre-qualification criteria.

A bidder participating in the procurement process shall possess the following minimum prequalification/ eligibility criteria

#### 3.1. Pre-Qualification for Bidder

SI	Parameter	Specific Requirements	Documents
1.	Legal Entity	<p>The Bidder should be an established Company registered under the – Indian Companies Act, 1956/2013, or partnership firm register under LLP Act, 2008 since last 10 years as on 31<sup>st</sup> March 2019.</p> <p>NB: - In case any bidder has undergone restructuring (merger, demerger, hive off, slump sale etc.), bid submitted by such bidder who has acquired a Company/Division of a company shall also be considered for evaluation if the eligibility and technical evaluation criteria is met jointly between the bidder and the Company/Division acquired.</p>	<p>Valid documentary proof of: Certificate of incorporation Certificate of Commencement Certificate consequent to change of name if applicable</p> <p>NB: Business Transfer Agreement (BTA) or Board resolution of both company or valid order of merger &amp; acquisition from ROC and/or Court. Credentials of its erstwhile / current entity provided sufficient documentary proof should be submitted with the bid to evince that such credentials have accrued to / transferred to / are in the name of the bidding entity and the bidding entity is authorized to use such credentials.</p>
2.	Financial Turnover	<p>Annual Turnover of the Bidder during the last three financial years, as per the last published audited balance sheets), should be more than (INR) 550 Crores each year as on 31<sup>st</sup> March 2019.</p> <p>NB: - In case Bidder is a wholly owned subsidiary, the financial experience of Parent company would be</p>	<p>CA Certificate for Net Worth with CA’s Registration No or Seal and Copy of audited profit and loss account and balance sheet of the last three financial years.</p>

SI	Parameter	Specific Requirements	Documents
		considered for eligibility, provided the parent company operates in similar field of business.	
3.	Net Worth	<p>The net worth of the Bidder should be Positive for last three years, as on 31<sup>st</sup> March 2019.</p> <p>NB: - In case Bidder is a wholly owned subsidiary, the financial experience of Parent company would be considered for eligibility, provided the parent company operates in similar field of business.</p>	Copy of audited profit and loss account/ balance sheet of the last three financial years, highlighting the requisite figure related to positive net worth and profitability.
4.	Certifications	<p>The Bidder must have following Certificates at the time of bidding,</p> <ol style="list-style-type: none"> <li>ISO 9001:2015</li> <li>ISO/IEC 20000 : 2018</li> <li>ISO/IEC 27001:2015</li> <li>ISO 27017 : 2015</li> </ol>	Copy of Valid Certificate.
5.	Project Experience	<p>During the last Five years, the Bidder should have implemented/completed and operated Data Centre projects for Central / State Governments, PSUs,PSE, Banking &amp; Financial Institutions, Telecom and IT companies in India that meets the below mentioned requirement :</p> <ol style="list-style-type: none"> <li>Single order of value 90 Crore or more; OR</li> <li>Two orders each having minimum value of 60 Crores or more; OR</li> <li>Three orders each having minimum value of 50 Crores or more</li> </ol> <p>(i) The orders should include Tier-III or Tier IV certified Data Centre consisting of installation, commissioning of Electrical Distribution &amp; Lighting, Electrical</p>	Copy of work order(s) / Purchase Order/ Completion Certificate/ contract agreement. Supported with relevant documentary evidences for the design parameters and the completion or Go Live or FAT certificates by the customer.

SI	Parameter	Specific Requirements	Documents												
		<p>Substation, DG sets with HSD tank, Precision AC/ Chiller Plant, UPS System, Fire Detection &amp; suppression system, Access Control and CCTV, BMS System, Civil and Interiors etc. &amp; IT components such as SITC of server, storage &amp; backup system, cloud solution, network &amp; cyber security equipment etc. for the Data Centre;</p> <p>AND</p> <p>(ii) Operation &amp; Maintenance including FMS of the Data Centre as on last date of Bid submission</p>													
6.	DC Design certificate Experience	The Bidder should have design experience of certification of at least one (1) Tier-III Data Centres (Design & Built) certified by Uptime Institute experience of certification should be of PSU/PSE/ Banks / Financial Institutions/ Telecom/ SDCs/ NDCs.	Copy of Tier III Certificate along with PO / Contract. Supported with relevant documentary evidences for the design parameters and the completion or Go Live or FAT certificates by the customer.												
7.	Technical Manpower	<p>The Bidder must have on its roll at least 200 technically qualified professionals in the Non-IT/ICT domains i.e. Electrical, HVAC systems, , networking, system software, systems integration, storage, Backup solution, cloud solution, Cyber security who have prior experience in providing the Data Centre Infrastructure maintenance services as on bid submission date.</p> <p>Bidder Must have at least following technical manpower on its role.</p> <p>i. 50 resources should be B.E/B. Tech/MCA or equivalent.</p>	<p>Certificate from bidder’s Head of HR Department for the 200 number of Technically Qualified professionals employed by the company in the following format.</p> <table border="1"> <thead> <tr> <th>Emp Name</th> <th>Qualification</th> <th>Certification</th> <th>Exp Year</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Emp Name	Qualification	Certification	Exp Year								
Emp Name	Qualification	Certification	Exp Year												



SI	Parameter	Specific Requirements	Documents
		<ul style="list-style-type: none"> <li>ii. 10 resources should be B.E/B. Tech (Electrical &amp; Mechanical)</li> <li>iii. At least 25 resources should be OEM certified.</li> <li>iv. At least five Project management professional with PMP or Prince-2 certified.</li> <li>v. At least five ITIL V3 (Intermediate level or higher) certified.</li> <li>vi. At least three CDCP/CDCS/ CDCE certified</li> <li>vii. At least one Data Centre Design Consultants having ATD (Accredited Tier Designer) certification from Uptime Institute.</li> </ul>	<p>HR certificate on company’s letterhead stating the points with employee Name, Qualification, Certification to be submitted along with copy of the relevant certificate</p>
8.	Mandatory Undertaking	<p>The Bidder shall: -</p> <ul style="list-style-type: none"> <li>a) Not be insolvent, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons;</li> <li>b) Not have, and their directors and officers not have, been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of five years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings;</li> <li>c) Not blacklisted with any of the State/Central Government or any government agency as on the date of submission of the bid.</li> </ul>	<p>Self-Certification/ Declaration duly signed by authorized signatory on company letter head.</p>

### 3.2. Submission of the Proposal

1. The proposal shall be submitted online in two parts in, Part-I “Technical cum General Bid” and Part-II “Commercial Bid”. Technical cum General Bid will consist of two parts; “Pre-Qualification Bid” & “Technical Proposal”. Technical Bid proposal will be provided as per format in [Proforma-4](#) and Commercial Bid will only consist of the commercial proposal as per format in [Proforma-25](#): Format for Financial Quotations
2. The bidders must submit their responses as per the format given in this RFP, in the following manner, which must be properly flagged to distinguish the required enclosures.

<b>Prequalification Bid</b>	
<b>Technical Proposal</b>	
<b>Commercial Proposal</b>	

3. The proposal should be signed by an authorized signatory (having power of attorney/authorized by board resolution) on each page of the proposal document including enclosures.
4. **Copy of board resolution and / or power of attorney shall be submitted along with technical proposal. Failing of which the Bid will be rejected.**
5. The proposal shall contain no interlineations, erasures or overwriting, in order to correct error made by the Bidder. All corrections shall be done & initialed by the authorized signatory after striking out the original words / figures completely.
6. The Bidder should submit a hard copy of the bid along with original DD against RFP fee, BG against the EMD and copy of technical presentation on a CD/DVD/Flash drive in the following address, which should reach on or before the last date, and time of the bid submission as mention in Invitation of Bid section.

**General Manager (Admin)**

Odisha Computer Application Centre

N1/ 7D, Acharya Vihar Square, Near Planetarium,

PO: RRL, Bhubaneswar 751013.

Odisha, India

Ph: 0674-2582850/ 2588064

Website: [www.ocac.in](http://www.ocac.in)

7. The outer and inner envelopes shall indicate the name and address of the Bidder to enable the bid to be returned unopened in the case it is declared "late" pursuant, and for similar purposes.
8. Only detailed complete bids in the form indicated above shall be received prior to the closing time and date of the bids shall be taken as valid.
9. Please note that Prices should not be indicated in the Technical Proposal but should only be indicated in the Commercial Proposal. Any proposal with Commercial Proposal submitted along with Technical Proposal will be summarily rejected.
10. All the pages of the proposal must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the proposal.
11. The original proposal /proposal shall be prepared in indelible ink. It shall contain no interlineations or overwriting, except as necessary to correct errors made by the Bidder itself. Any such corrections must be initialed by the person (or persons) who sign(s) the bids.
12. All pages of the proposal including the duplicate copies, shall be initialed and stamped by the authorized person or persons who sign the proposal.

### 3.3. Deadline for Submission of Proposals

1. The proposal shall be submitted in hardcopy, along with RFP fee, EMD as BG and Technical Presentation in CD/DVD/Flash Drive must be submitted/sent at the specified address as mentioned above within the above date and time.
2. OCAC may, at its discretion, extend this deadline for any other administrative reason.

### 3.4. Late proposals

- Any proposal received by OCAC after the deadline for submission of proposals prescribed by OCAC, shall be rejected.

### 3.5. Proposal Prices

The prices indicated in the price schedule shall be entered in the following manner:

1. The total price quoted must be inclusive of cost of Non-IT and IT supply, installation, commissioning and supplying / providing hardware, licenses, software, services for installation, testing and commissioning of the Solution and support, all applicable taxes, duties, levies, charges etc., it should also include the cost of incidental services such

as transportation, insurance, training, factory acceptance test, acceptance test at site, Certification, Periodic health check, operation and maintenance etc.

2. The cost of operation and maintenance of Non- IT infrastructure and IT systems for a period of FIVE (5) years after the date of Go Live.
3. The Bidder cannot quote for the project in part.
4. The Bidder may visit the all proposed site/location, which will be part of OSDC 2.0 at Bhubaneswar before bidding to assess the actual physical & technical requirement. Site visit may be facilitated on mail request to the Contact Officer as mentioned in invitation of bid section.
5. The bidder must submit a detailed Bill of material including Make & Model and Bill of quantity with prices of each component.
6. OCAC will have in its discretion to increase and decrease in quantity and items in case of need arises.
7. Bidder to offer buys back prices for the items those are getting replaced by new one. The buyback prices will be a part of commercial evaluation.

### 3.6. Earnest money deposit

1. Bidders shall submit, an EMD of Rs. 2,00,00,000.00 (Two Crore only), in the form of bank guarantee issued by any nationalized/scheduled commercial bank in favor of OCAC, payable at Bhubaneswar, and should be valid for minimum 180 days from the last date of the submission of Bid.
2. EMD of all unsuccessful bidders would be refunded by OCAC within 60 days after selection of successful Bidder. The EMD of successful Bidder would be returned upon submission of Performance Bid Security as per the format provided in [Proforma-24](#).
3. EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.
4. The proposal submitted without tender fee and EMD in the prescribed format mentioned above, shall be summarily rejected.
5. The EMD may be forfeited:
  - a. If a Bidder withdraws its proposal within the validity period.
  - b. In case of a successful Bidder, if the Bidder fails to sign the contract in accordance with this RFP.
  - c. Fails to deliver as per the Terms & conditions of RFP & deliverables.
  - d. Any material breach of contract

### 3.7. Bid Validity Period

- The EMD submitted along with the bid will remain valid for entire validity period of the bid as mentioned in the fact sheet.

- In exceptional circumstances, prior to expiry of the bid validity period, OCAC may request the bidders to extend the period of validity for a specified additional period at bidder's cost. The request and the responses to the request shall be made in writing. A bidder may refuse the request without risking forfeiting the EMD, but in this case, the bidder will be out of the competition for the award. Bidder agreeing to the request will not be required or permitted to modify its bid, but will be required to ensure that the bid remains secured for a correspondingly longer period.
- On completion of the validity period, unless the Bidder withdraws his bid in writing, it will be deemed valid until such time that the Bidder formally (in writing) withdraws bid.

### 3.8. Compliant /Completeness of response

Bidders are advised to study, examine all instructions, forms, appendices, terms, conditions and deliverables in the RFP document. Failure to furnish all information required by the RFP documents or submission of a RFP offer not substantially responsive in every respect to the RFP documents will be at the bidder's risk and may result in rejection of its RFP offer.

The RFP offer is liable to be rejected outright without any intimation to the bidder if complete information as called for in the RFP document is not given therein, or if particulars asked for in the forms / Proforma in the RFP are not fully furnished.

Bidder must:

- Include all documentation specified in this RFP, in the bid.
- Follow the format of this RFP while developing the bid and respond to each element in the order as set out in this RFP.
- Comply with all requirements as set out within this RFP.

### 3.9. Pre-bid Meetings Clarification

OCAC shall organize a virtual pre bid meeting on the scheduled date, time and venue as mentioned in Invitation of Bid section, at OCAC Building, Bhubaneswar. OCAC may or may not incorporate any changes in the RFP based on acceptable suggestions received during the Pre-Bid Conference. The decision of OCAC regarding acceptability of any suggestion/request shall be final in this regard and shall not be called upon to question under any circumstances. The prospective bidders shall submit their queries in writing only in prescribed format below not later than date and time indicated in sheet.

Representatives from any OEM shall not be allowed to be part of the pre-bid meeting. OEM should also not accompany any of their system integrator or partners, and are expected to submit their queries through partners or directly via electronic form in the prescribed format as below for seeking clarifications.

Sl. No	Page No	Clause No	Clause header	Clause details as in RFP	Query/ Clarification Required	Justification/Reason for changes required (If any)
--------	---------	-----------	---------------	--------------------------	-------------------------------	--

At any time prior to the last date of submission of proposal, OCAC may for any reason be able to modify the RFP.

Any modifications in RFP or reply to queries shall be hosted – <http://www.ocac.in> & [www.odisha.gov.in](http://www.odisha.gov.in)

- OCAC at its discretion may extend the last date for the receipt of proposals.
- Once the similar queries shall be answered, same queries will not be entertained further.
- It is expected that the bidder shall do their own due-diligence on the question they may ask. Any changes sought must be with proper justification. Any statements such as 'specification/requirement is not vendor neutral' OR 'it implies to single OEM' or any such statement similar to this, must be asked with adequate and credible proof and justification, else such queries will not be accepted.

### 3.10. Responses to pre-bid queries and issue of corrigendum

1. Bidder may seek clarification on this RFP document not later than the date specified in the Invitation of Bid section. OCAC reserves the right to not to entertain any queries post that date and time. The bidder are requested to submit their queries in MS -Word as well as MS-Excel editable format.
2. At any time prior to the last date for receipt of bids, OCAC may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the RFP document through a corrigendum.
3. Any modifications of the RFP Documents, which may become necessary as a result of the Pre-Bid queries, shall be made by OCAC exclusively through a corrigendum. Any such corrigendum shall be deemed to be part of this RFP and incorporated into this RFP. However, in case of any such amendment, the bid submission date may be extended at the discretion of OCAC.
4. The corrigendum or clarifications (if any) to the queries from any bidder will be published on the website, <http://www.ocac.in> & [www.odisha.gov.in](http://www.odisha.gov.in) in form of modified RFP/corrigendum etc.
5. In order to provide prospective bidders reasonable time for taking the corrigendum/modifications into account, OCAC may, at its discretion, extend the last date for the receipt of Bids.

6. It is the responsibility of the bidder to check the above websites time to time for updates.

### 3.11. Amendment of Proposals

- RFP Proposals once submitted cannot be amended. However, in case of some administrative exigencies, OCAC may decide to take fresh proposals from all the bidders before opening of the Technical Proposal.
- OCAC in its discretion may ask for clarification in terms of letter, declaration, datasheets, brochures etc during technical evaluation. It will be binding on the bidders to submit the same

### 3.12. Opening of proposals by OCAC

The date and time for opening of proposals and technical presentation will be decided and notified by OCAC through the website of [www.ocac.in](http://www.ocac.in). The evaluation committee authorized by OCAC will be entitled for proposal opening in the presence of bidders or their representatives who may be present at the time of opening. The bidder's representatives (maximum two) should carry the identity card or a letter of authorization from the bidding firms to identify their employer for attending the opening of the proposal. In order to assist in the examination, evaluation and comparison of proposals, OCAC may at its discretion ask the bidder for a clarification regarding its proposal. The clarification shall be given in writing, but no change in the price or substance of the proposal shall be sought, offered or permitted.

### 3.13. Evaluation Procedure

1. OCAC may constitute an Evaluation Committee to evaluate the responses of the bidders.
2. The Evaluation Committee constituted by OCAC shall evaluate the responses to the RFP and all supporting documents / documentary evidence. Inability to submit requisite supporting documents / documentary evidence, may lead to rejection.
3. The interpretation of the bids and the decision made by the Evaluation Committee in the evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of evaluation with the committee.
4. The Evaluation Committee may ask for meetings with the bidders to seek clarifications on their bids.

5. The Evaluation Committee reserves the right to reject any or all bids on the basis of any deviations.
6. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.
7. Initial Proposal scrutiny will be held and incomplete details as given below will be treated as non-responsive. If Bids;
  - a. Are submitted without tender fee or EMD in prescribed format.
  - b. Are not submitted as specified in the RFP document.
  - c. Received without the Letter of Authorization (Power of Attorney)
  - d. Are found with suppression of details
  - e. With incomplete information, subjective, conditional offers and partial offers submitted
  - f. Submitted without the documents requested in the Proforma.
  - g. Have non-compliance of any of the clauses stipulated in the RFP
  - h. With lesser validity period
8. Evaluation Committee will prepare a list of responsive bidders, who comply with all the Terms and Conditions of the RFP. All eligible bids will be considered for further evaluation by a Committee according to the Evaluation process defined in this RFP document. The decision of the Committee will be final in this regard. All responsive Bids will be considered for further processing as below:
  - a. Evaluation committee will examine the bids to determine whether they are complete, whether any computational errors have been made, and whether the bids are generally in order. The interpretations made by the evaluation committee will be final and binding on the bidders.
  - b. Reasonableness of Prices: Prices quoted by bidders must be reasonable with prevalent market rates. AHR (Abnormally High Rates) and ALR (Abnormally Low rates) shall not be accepted and OCAC shall have the right to reject the bid.
  - c. In a case where the item is mentioned in the BOQ/BOM/Price bid but the prices are not mentioned against the item, then OCAC shall have the discretion to consider the highest cost among all the qualified bidder for that item for calculation to reach the total prices of the bidder. However the bidder has to execute the item at free of cost only.
  - d. In case an item has been left out in the BOQ/BOM/Price bid by a particular bidder but required for the successful implementation of project and/or it is mentioned in the solution document of the bidder, OCAC will have the right to reject the bid OR ask the bidder to supply the item free of cost.



- e. It is mandatory for bidder to submit detailed BOQ and BOM (Bill of material with quantity) as unpriced bid in technical bid. Any discrepancy in price and unpriced bid will lead to disqualification of the bid OR OCAC will have the right to consider the highest amongst the BOQ/BOM and the price bid.
- f. In case of no price quoted or Zero price quoted against an item by a bidder, price for the item will be loaded with highest prices quoted amongst all the other bidders for that item for evaluation purpose. However, the bidder has to complete the SITC for the item at zero cost.
- g. In case of a situation where the bidder has quoted abnormally low quantity or abnormally high quantity for an item, OCAC will have the rights to ask for an explanation during technical evaluation stage. The bidder will be given chance to increase or decrease the quantity as per the solution the bidder would propose and accepted OCAC. This will not be applicable for the quantity mentioned against items that is already asked in the tender. Accordingly during commercial evaluation the prices will be calculated for revised quantity submitted by bidder.
- h. Arithmetical errors will be rectified on the following basis:
  - If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected.
  - If there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected.
  - If the Bidder does not accept the correction of the errors, his proposal will be rejected.
  - If there is a discrepancy between words and figures, the amount in words will prevail.
- i. OCAC may conduct clarification meetings with each or any Bidder to discuss any matters, technical or otherwise. Result of such meeting/ clarification may be published on specified website; however, no material changes in the bid shall be permitted.
- j. Further, the scope of the evaluation committee also covers taking any decision with regards to the RFP Document, execution/ implementation of the project including management period.
- k. Proposal shall be opened in the presence of bidders representatives who intend to attend at their cost. The bidders' representatives who are present shall sign a register giving evidence of their attendance.
- l. Proposal document shall be evaluated as per the following steps.

- Preliminary Examination of Eligibility Criteria documents: The Eligibility document will be examined to determine whether the Bidder meets the eligibility criteria, whether the proposal is complete in all respects, whether the documents have been properly signed and whether the bids are generally in order. Any bids found to be non-responsive for any reason or not meeting the minimum levels of the performance or eligibility criteria specified in various sections of this RFP Document will be rejected and will not be considered further.
- Technical Evaluation: A detailed evaluation of the bids shall be carried out in order to determine whether the bidders are competent enough and whether the technical aspects are substantially responsive to the requirements set forth in the RFP document. Bids received would be assigned scores based on the parameters defined in the table.
- The technically qualified bidders shall be invited during opening of the commercial bids and subsequently commercial evaluation shall be carried out.

### 3.14. Technical Bid Evaluation Scoring Matrix

#### Tender Evaluation Methodologies

The evaluation has been divided in three basic categories i.e.

- (a) Organizational strength and Project Experience Evaluation
- (b) Technical Evaluation
- (c) Technical Presentation

The bid evaluation will be carried out as per the below details;

Sl.	Criteria	Scores
1	Organizational strength and Project Experience	20
2	Technical (IT and Non-IT) Offerings	60
3	Technical Presentation	20
<b>Total</b>		<b>100</b>

#### A. Organizational Strength and Project Experience – 20 Marks

Sl.	Description	Max. Score	Scoring Mechanism	Credential Required
1	<b>Turn over:</b> Annual Turn Over per annum of Bidder for last 3 years as mentioned in eligibility criteria, minimum 550 Crores.	3	>= 550 Crores- <650 = 1 Marks  >651 Crores and <=1000 Crores = 2 Marks  > 1000 Crores = 3 Marks	Copy of audited Balance Sheets and Profit and Loss (P/L) statement for last 3 years 2018-19, 2017-18, 2016-17 up to March 31 <sup>st</sup> 2019.
2	<b>Project Experience:</b> During the last Five years, the Bidder should have implemented/completed and operated Data Centre projects for Central / State Governments, PSUs, PSE, Banking & Financial Institutions, Telecom and IT companies in India. a. Single order of value 90 Crore or more; OR b. Two orders each having minimum value of 60 Crores or more; OR c. Three orders each having minimum value of 50 Crores or more	7	>=90 crore - 1 order OR >=60 crore - 2 orders OR >=50 crores -3 orders = 5 Marks  >=90 crore -2 orders OR >=60 crore-4 orders OR >=50 crores -6 orders = 7 Marks	Copy of Work Order / Agreement / Work Completion/ In progress Certificate

3	<b>Implementation Experience:</b> Bidder's experience in Large Scale implementation of IT System Integration project with a min value of Rs. 90 Crore or above.	7	>=90 crore = 3 Mark >90 crore < 100 crore = 5 Marks >=100 crores = 7 marks	Copy of Work Order / Agreement / Work Completion/ In progress Certificate
4	<b>Facility Management Service (FMS) Experience:</b> Bidder's experience in providing facility management services to scheduled bank/PSU/Govt. Organization, quantified in terms of number of projects will be evaluated; project considered for evaluation should have project cost more than Rs. 5 Crore.	3	>=5 crore = 1 Mark >5 crore <7.5 Crore = 2 Mark >7.5 crores = 3 Mark	Copy of Work Order / Agreement / Work Completion/ In progress Certificate
<b>Total</b>		<b>20</b>		

**B. Technical Evaluation for Non-IT Devices: (Total Score: 25)**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
1	Critical UPS	2	AC Efficiency	>96%	0.5
				95% to 96%	0.15
			IGBT Inverter Level	> 3	0.4
				2 to 3	0.15
			Power Module Rating	>25 KW	0.4
				<25 KW	0.15
			UPS System	UL/CE Listed	0.4
				Non UL/CE Listed	0.15
LIB System(Cell and Module and System)	UL Listed	0.3			
	Non UL Listed	0.25			

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
2	Non- Critical UPS	1	AC Efficiency	>95%	0.6
				94% to 96%	0.2
			UPS Unity Power factor 20 kVA = 20 KW	Available	0.4
				Non Available	0.2

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
3	In Row PAC	2	Control of Refrigerant through Electronic Expansion during Dehumidification process	Available	1
				Non Available	0.5
			Air Quantity	>=100 CFM/KW	1
				<100 CFM/KW	0.5

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
4	PAC	2	SHR	>=0.92	0.5
				<0.92	0.25
			Installation base in India	>=100	1
				<100	0.5
			Manufacturing experience in India	>=10 years	0.5
				<10 years	0.25

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
5	Diesel Generator	2	Engine volumetric capacity	> 50 Litres.	0.8
				=50 Litres.	0.4
			Voltage Regulations	Less than +/- 1 %	0.4
				= +/- 1 %	0.08
			Service Centre in Bhubaneswar	Yes	0.4
				No	0.08
			Fuel efficiency@75% load	<275 Ltr per hour	0.4
				>275 Ltr per hour	0.08

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
6	Track Bus way System	1	Polarized Plugin Units	Yes	0.5
				No	0.1
			Installations in India	>5 nos.	0.5
				<5 nos.	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
7	MV Panels	0.5	Installation of similar From 4b panels in eastern region. Documentary evidence required	>5 Installations	0.25
				<=5 Installations	0.125
			Service Centre at Bhubaneswar	Available	0.25
				Not Available	0.125

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
8	Passive Cabling	0.5	The complete solution should be intelligent from day 1 of installation.	Yes	0.25
				No	0
			Installation of similar products in at least 5 Data Centres (minimum 1000 copper + Fiber ports) across India in last 2 years. Documentary evidence to be submitted.	>=5 Data Centre with minimum 1000 copper + fiber ports in last 2 years	0.25
				1-4 Data Centre with minimum 1000 copper + fiber ports in last 2 years	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
9	DCIM	0.5	No. of implementations in PSUs/PSBs/ Government organizations	>5	0.25
				Between 3 to 5	0.1
			User Defined Reports and Dashboard	Yes	0.25
				No (Fixed Dashboard)	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
10	IPDU	1.5	No. of iPDUs that can be cascaded / IP Aggregation (resulting in savings of Copper Ports)	>=40	0.75
				Environmental Sensor Integration	Temp. + Humidity + Dew point + Airflow
				Temp. + Humidity	0.375
				None	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
11	IT Racks	1.5	Load Bearing capacity (High Density)	>1200 Kgs	0.75
			Rack Perforation level	>75%	0.75
				63-75%	0.375

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
12	Critical Rack Access Control	1	Capability of Fire Emergency Lockout	Yes	0.5
				Yes	0.5
			Secure event Logging in case of Power Failure	No	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
13	HT Panels	1	Service centre in Bhubaneswar	Yes	0.25
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.25
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
14	Transformer	1	On load tap changer (OLTC) and remote tap Change control (R.T.C.C.) panel	Yes	0.25
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.25
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
15	Fire Alarm System	1.5	Service Centre in Bhubaneswar	Yes	0.5
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.5
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
16	Gas Based Suppression System	1.5	Service Centre in Bhubaneswar	Yes	0.5
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.5
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
17	Access Control System	1	Service Centre in Bhubaneswar	Yes	0.34
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.33
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.33
				No	0

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
18	HSSD	1.5	Service Centre in Bhubaneswar	Yes	0.5
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.5
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0



Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
19	CCTV	1	Service Centre in Bhubaneswar	Yes	0.34
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.33
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.33
				No	0

**C. Technical Evaluation for IT Devices: 35 Marks**

Sl.	Name of the Device	Max. Score	Parameter / Specification	Score
1	Server Type-1 (Rack Server)	2.5	Processor Type-1 should have 2 x 16 cores or higher, minimum 2.8 GHz clock rate or more.	1.25
			Processor Type-1 should have 2 x 16 cores and less than 2.8 GHz clock rate	1
			Processor Type-2 should have 2 x 28 cores or higher, minimum 2.1 GHz clock rate and more.	1.25
			Processor Type-2 should have 2 x 28 cores less than 2.1 GHz clock rate.	1

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
2	Core Router	2.5	The Router should provide minimum aggregate throughput bandwidth of 5 Gbps scalable up to 20 Gbps or more	2.5
			The Router should provide minimum aggregate throughput bandwidth of 5 Gbps scalable up to 20 Gbps	2

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
3	Spine Switch	2.5	Shall offer minimum of 30 Tbps or more and wired speed non-blocking forwarding performance. from day-1.	2.5

			Shall offer minimum up to or less than 30 Tbps or more per-slot bandwidth from day-1.	2
--	--	--	---	---

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
4	Leaf Switch type-1 (Fibre)	2.5	Switch Shall offer routing/switching capacity of minimum of 2.66 Tbps or more, speed non-blocking forwarding performance.	1.5
			Switch Shall offer routing/switching capacity of minimum of 2.66 Tbps or less, speed non-blocking forwarding performance.	1
			Support for 10G, 25G, 40G, and 100G from day-1	1

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
5	Access Switch (Copper)	2.5	Shall have routing/switching capacity of 1.25 Tbps or more forwarding performance.	2.5
			Shall have routing/switching capacity of 1.2 Tbps or less forwarding performance.	2

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
6	Management Switch -2	2.5	Shall have routing/switching capacity routing/switching capacity of minimum of 1 Tbps or more forwarding performance.	2.5
			Forwarding performance below 1 Tbps forwarding performance.	2

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
7	Enterprise Storage	2.6	Enterprise Class Storage System and supplied with 1PB or more usable capacity of all SSD/ Flash /FMD.	1
			Enterprise Class Storage System and supplied with less than 1PB usable capacity of all SSD/ Flash /FMD.	0.8
			The enterprise storage array must be proposed with a minimum of four controllers/directors & should be scalable up to eight	1

			controllers/directors as a single array (serial number/asset).	
			The enterprise storage array must be proposed with a minimum of four controllers/directors & should be scalable less than eight controllers/directors as a single array (serial number/asset).	0.8
			The designed IOPs for 30:70 Write: Read for the above systems for RAID 6 should be minimum 1million IOPS with 8K block size from SSD tier	0.6
			The designed IOPs for 30:70 Write: Read for the above systems for RAID 6 is less than 1million IOPS with 8K block size from SSD tier	0.4

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
8	Tape Library	2.6	Shall support Native data capacity of more than 3PB (uncompressed) expandable to more than 4 PB (2.5:1 compressed) when fully populated, using LTO-8 or higher	2.6
			Shall support Native data capacity of more than 3PB (uncompressed) expandable to less than 4 PB (2.5:1 compressed) when fully populated, using LTO-8	2

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
9	Link Load Balancer	2.5	The appliance should have 10 Gbps or more throughput from day one	2.5
			The appliance has less than 10 Gbps throughput from day one	2

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
10	Next Generation Firewall (NGFN)	2.6	The proposed OEM must have completed NSS Labs' NGFW Methodology testing with a minimum exploit blocking rate of 95% and must have a track record of continuous improvement in threat detection (IPS).	1
			Minimum exploit Blocking rate < 95%.	0.8
			Proposed appliance must support at least 6 million concurrent sessions and 300,000 new	1

			connections per second from day one.	
			Proposed appliance support less than 6 million concurrent sessions and 300,000 new connections.	0.8
			A minimum storage capability of 2TB (should be on a separate management appliance) need to be provided as part of the solution for logging and reporting.	0.6
			Storage capacity < 2TB	0.4

D.

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
11	AAA	2.6	Solution shall be provided with required licenses for minimum 2000 concurrent sessions for AAA and TACACS+ access on Day 1. Solution shall be scalable up to 4,000 concurrent sessions without any hardware change.	2.6
			Solution shall be provided with required licenses for less than 2000 concurrent sessions for AAA and TACACS+ access on Day 1.	2

E.

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
12	DDOS Solution	3	Solution should Provide Minimum 20 Gbps mitigation throughput.	1.5
			<20 Gbps throughput	1.25
			Solution should provide Min 18 Gbps SSL throughput	1.5
			<18 Gbps SSL throughput	1.25
Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
13	SDN Controller	2.6	The SDN solution should support VMs (running on ESXi, KVM / Hyper-V/RHEV) Minimum 2 or more platforms must be supported	2.6
			The Solution should support VMs (running on ESXi, KVM)	2

F.

Sl.	Name of the Device	Max. Score	Parameter/ Specification	Score
14	Anti-APT	1.5	Appliance must be able to handle minimum of 1 Gbps or more of traffic capacity for inspection	1.5
			Appliance must be able to handle minimum of 1 Gbps of traffic capacity for inspection	1

## G. Technical Presentation -20 Marks

The technical presentation should be professional and should contain below details and not limited to;

Bidder's understanding of the project & scope of work – 5 Marks

Solution Architecture & Design (Non-IT & IT) – 5 Marks

Approach & Methodology – 3 Marks

Project Plan & Project Team's Experience – 3 Marks

Operation and Maintenance Plan – 4 Marks

Note:

1. This is for vendor's internal reference. Need not be submitted with Bid.
2. Vendors need to provide relevant credentials for all of the above points, for scoring.
3. OCAC reserves the right to verify the correctness of documentary evidence furnished by the bidder for successful operation and performance of qualifying projects and Bidder shall arrange permission for the same
4. The solution, as demonstrated, will be scored on a pre-set questionnaire.
5. The product technical architecture, supporting documentation etc. describing the various technical parameters need to be provided.
6. The proposed FM plan, as part of vendor proposal, will be evaluated.
7. The overall proposal, implementation methodology, adherence to project plan etc. will be evaluated.
8. **Bidder's DC Build experience of own in-house Data Centre or own Internet Data Centre for commercial use shall not be accepted.**

### 3.15. Evaluation of Bids and Award of Contract.

Technical Evaluation: A detailed evaluation of the bids shall be carried out in order to determine whether the bidders are competent, enough and whether the technical aspects are substantially responsive to the requirements set forth in the RFP document. Bids received would be assigned scores based on the parameters defined in the table.

Every bidder will be given a time slot of 60 minutes to present the Approach and Methodology, components and resources proposed for the project. The bidder who score minimum cut-off marks 75 or more will be qualified for the evaluation of their commercial bids.

The technically qualified bidders shall be invited during opening of the commercial bids and subsequently commercial evaluation shall be carried out.

Evaluation of bids would be done on **QCBS (Quality and Cost Based Selection)** criteria as detailed. The bidder shall have to score at least 70 marks in Technical Score as per "Evaluation

and Selection Matrix” for being eligible for opening of financial proposal. The bids quoted as per the commercial bid format will be considered for commercial evaluation.

The Evaluation Methodology adopted will be **Quality cum Cost Based System (QCBS)** method of evaluation where Technical Bid Score will get a weightage of 60% (denoted by ST) and Commercial Bid Score a weightage of 40% (denoted by SF).

**A. Calculation of Technical Score (ST)**

T = Technical Marks obtained by the Individual Bidder.

Tmax = Highest Technical Marks obtained by individual bidder.

ST = Technical Score obtained by the Individual Bidder

**Calculation of Technical Score (ST)**

$ST = 100 \times (T/T_{max})$  (rounded off to 2 decimal places)

**B. Calculation of Financial Score (SF)**

F = Total Financial Bid amount quoted by individual Bidder

Fmin= Lowest Total Financial Bid amount quoted by individual Bidder.

SF = Financial Score obtain by the Individual Bidder

**Calculation of Financial Score (SF)**

$SF = 100 \times (F_{min}/F)$  (rounded off to 2 decimal places).

**Calculation of Final Composite Score (S)**

The Final Composite Score (S) shall be computed for each firm by assigning 60% weightage to the Technical Score (ST) and 40% weightage to Financial Score (SF) using the formula given below:

**Calculation of Final Score (S)**

**$S = (ST \times 0.6) + (SF \times 0.4)$**  (rounded off to 2 decimal places)

Bidder with the highest final composite score will be awarded the contract. In case of a “tie” in the final composite score between two bidders, the bidder with the higher Technical Score will be invited for negotiations and selected to be awarded.

### 3.16. Deviations and Exclusions

Bids shall be submitted strictly in accordance with the requirements and terms & conditions of the RFP. The bidder shall submit a No Deviation Certificate as per the format specified in Proforma 16. The bids with deviation(s) are liable for rejection.

### 3.17. Rejection of Bids

The bids shall be rejected on the following grounds:

1. In the event of any assumptions, presumptions, key points of discussion, recommendation or any points of similar nature submitted along with the Bid, OCAC reserves the right to reject the Bid and forfeit the EMD
2. If any of the eligibility criteria as per the Pre-qualification criteria is not met
3. EMD/ RFP fee not submitted
4. If RFP terms and conditions are not met
5. Commercial bid is enclosed with the same document as technical bid.
6. If Bidder gives incorrect/misleading/ fraudulent information in the bid.
7. Failure to furnish all information required in the RFP document.
8. Canvassing in any form in connection with the bids
9. If the bid is incomplete /partial bid/ conditional/unclear in any form, has deviations from the terms and conditions of RFP
10. Information submitted in technical bid is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period if any
11. Bids submitted after due date and time.
12. Bids are submitted through Telex/Fax/ e-mail
13. Erasure and/or overwriting
14. Bids not signed by authorized signatory or without power of attorney
15. Multiple makes of items.

### 3.18. Notification of Acceptance of Proposal

Prior to the expiry of the period of Proposal validity, OCAC will notify the selected Bidder in writing by speed post or Fax or email that its proposal has been accepted and has been selected to do the project.

## 4. General Conditions of Contract

### 4.1. Definition of Terms

**a. "Acceptance of System"** The system shall be deemed to have been accepted by Client, subsequent to its installation, rollout and deployment of the trained manpower, when all the activities as defined in Scope of Work have been successfully executed and completed to the satisfaction of the Client as evidenced by an Operational Acceptance Certificate.

**b. "Applicable Law(s)"** Any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Contract and during the subsistence thereof, applicable to the project.

**c. "Approvals"** OCAC shall extend necessary support to SI to obtain, maintain and observe all relevant and customary regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "Approvals") necessary for SI to provide the Services. The costs of such Approvals shall be borne by SI. Both Parties shall give each other all co-operation and information reasonably.

**d. "Bidder"** shall mean organization submitting the proposal in response to this RFP.

**e. "Client"** means the Odisha Computer Applications Centre (OCAC). The project shall be executed in Bhubaneswar and shall be owned by Odisha Computer Applications Centre (OCAC and E&IT Dept., Govt. of Odisha.

**f. "Clause"** means a clause of the GCC, as may be supplemented

**g. "Contract"** means the Contract Agreement entered into by the Client and SI, together with the entire contract documentation specified therein. The Contract Agreement and the Contract Documents shall constitute the Contract and the term "Contract" shall in all such documents be construed accordingly.

**h. "Contract Agreement"** means the agreement entered between the Client and the SI using the form of Contract Agreement contained in the Contract Documents. The date of the Contract Agreement shall be recorded in a signed form.

**i. "Contract Value"** means the price payable to SI under this Contract for the full and proper performance of its contractual obligations.

**j. Commercial Off-The-Shelf (COTS)"** refers to software products that are ready-made and available for sale, lease, or license to the general public.



**k. "Day"** means a working day as per the calendar of Government of Odisha/ Odisha Computer Applications Centre (OCAC)

**l. "Data Centre Site"** means the Data Centre sites including their respective Data Centre space wherein the delivery, installation, integration, management and maintenance services as specified under the Scope of Work are to be carried out for the purpose of this Contract.

**m. "Deliverable"** means a work product (including materials, equipment, installations, reports, software, know-how, design, drawings, diagrams, maps, models, specifications, analysis, solutions, data base, programmes technical information, data and other documents) to be prepared and submitted by the SI as a part of the Service, in accordance with the terms of this Contract and the term "Deliverables" shall be construed accordingly. The list of Deliverables to be provided by the SI is set out in scope of work.

**n. "Document"** means any embodiment of any text or image howsoever recorded and includes any data, text, images, sound, voice, codes, databases or any other electronic documents as per Information Technology Act, 2000 read along with the rules and regulations made thereunder.

**o. "Effective Date"** This Contract shall come into force and effect on the date on which the Contract Agreement has been duly executed for and on behalf of the Client and the SI.

**p. "Force Majeure"** shall have the meaning ascribed to it in GCC Clause 4.18.

**q. "GoI"** means Government of India.

**r "GoO"** means Government of Odisha.

**s. "Go-Live"** means commissioning of the project after commencement of all Data Centre components, including training as per Scope of Work mentioned in RFP. SI should have the approval from the Client for user acceptance testing before Go-Live.

**t. "Goods"** means all of the equipment, sub-systems, hardware, software, products accessories, software and/or other material/items which SI is required to supply, install and maintain under the contract.

**u. "LoA"** means the letter of award issued to the selected Bidder pursuant to the RFP for its appointment as the SI.

**v. "Performance Bank Guarantee"** means the successful bidder has to submit 10% of the total project value as Performance Bank Guarantee to OCAC within 30 days of Letter of intent / Award

of project contract. The Performance Bank Guarantee (PBG) submitted by the successful bidder should have a validity of at least 90 days beyond the contract period.

**w. "OEM"** means the Original Equipment Manufacturer of any equipment/system/software/product or other Goods to be supplied by the MSI to the Client as a part of its Scope of Work.

**x. "Services"** means the work to be performed by the SI pursuant to the RFP and the contract to be signed by the Parties in pursuance of any specific assignment awarded by the Client.

**y. "Service Level(s)"** means the service level parameters and targets and other performance criteria which will apply to the Services and Deliverables as described in the RFP and the Service Level Agreement.

**z. "Service Level Agreement or SLA"** means the service level agreement specified in the RFP.

#### 4.2. Total Responsibility

Bidder should issue a statement undertaking total responsibility for the defect free operation with effective SLAs of the proposed solutions as per the format mentioned in Proforma 3.

#### 4.3. Right to terminate the process

- OCAC may terminate the RFP process at any time and without assigning any reason. OCAC make no commitments, express or implied, that this process will result in a business transaction with anyone.
- This RFP does not constitute an offer by OCAC. The bidders' participation in this process may result OCAC selecting a Bidder to engage towards execution of the contract.

#### 4.4. Language of Proposal & Correspondence

The proposal will be prepared by the Bidder in English language only. All the documents relating to the Proposal (including brochures) supplied by the Bidder should also be in English, and the correspondence between the Bidder & OCAC shall be in English language only. The correspondence by Fax / E-mail must be subsequently confirmed by a duly signed copy (unless already signed digitally).

#### 4.5. OCAC's Right to accept and to reject any or all proposals

- Notwithstanding anything else contained to contrary in this RFP Document, OCAC reserves the right to accept or reject any Bid or to annul the bidding process fully or partially or modifying the same and to reject all Proposals at any time prior to the award of work, without incurring any liabilities in this regard.
- OCAC may terminate the RFP process at any time and without assigning any reason. OCAC makes no commitments, express or implied, that this process will result in a business transaction with anyone.
- This RFP does not constitute an offer by OCAC. The bidder's participation in this process may result OCAC selecting the bidder to engage towards execution of the contract.

#### 4.6. Modification and withdrawal of bids

- The Bidder may be allowed to modify or withdraw its submitted proposal any time prior to the last date prescribed for receipt of bids, by giving a written notice to OCAC.
- The Bidder's modification or withdrawal notice shall be prepared, sealed, marked and dispatched in a manner similar to the original Proposal.
- Subsequent to the last date for receipt of bids, no modification of bids shall be allowed. No bid may be withdrawn in the interval between the deadline for submission of bids and expiration of the of bid validity period specified. Withdrawal of a bid during this period will result in Bidder's forfeiture of bid security/EMD.
- No written, oral, telegraphic or telephonic proposals modifications will be acceptable.

#### 4.7. Contacting OCAC

Any effort by a Bidder to influence the proposal evaluation, proposal comparison or contract award decisions at OCAC level may result in the rejection of the proposal.

#### 4.8. Knowledge of Site Conditions

The SI's undertaking of this Contract shall be deemed to mean that the SI possesses the knowledge of all data centre related requirements as stipulated in the Tender Document including but not limited to environmental, demographic and physical conditions and all criteria required to meet the design of the data centre.

#### 4.9. Failure to agree with terms & conditions of the contract

Failure of the SI to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event OCAC may award the contract to the next best value SI or call for new bids from the interested bidders or invoke the PBG of the most responsive SI. However, SI shall be allowed to submit minor

deviations without any cost implications and allowed for opportunity to mutually discuss its terms and conditions. The final decision in such an occurrence lies with OCAC.

#### 4.10. Governing Law & Jurisdiction

The Contract shall be governed by and interpreted in accordance with the laws of the India. The High Court of Judicature at Cuttack and Courts subordinate to such High Courts shall have exclusive jurisdiction in respect of any disputes relating to the tendering process, award of Contract and execution of the Contract.

#### 4.11. Termination and Effects of Termination

This Agreement shall be terminated by either party upon the happening of all or any of the following events:-

- Upon either Party being declared insolvent or bankrupt.
- Upon either Party committing a material breach or being in default of all or any of the major and significant terms, conditions, covenants, undertakings and stipulations of this Agreement. In case the material breach is remediable the aggrieved Party shall give notice in writing of such default in observance or performance of any of the terms or conditions of this Agreement, to the Party in default. If the Party in default effectively remedies such breach or default within the period, not being less than 60(sixty) days, designated by such notice then the Agreement shall remain in force. Where the default by the System Integrator is as a result of or consequent to technical non- feasibility, which requires to modify/alter the scope of work so as to replace the technical non-feasible deliverable , with a feasible deliverable, then such default shall not be considered a default by the System Integrator under the provisions of this clause
- By mutual agreement in writing between the parties.

1. Termination for Breach- In the event of the breach of any of the major and significant terms and conditions of this Agreement by the system integrator, OCAC shall be entitled to terminate this agreement by giving 60 days' notice. The decision of OCAC as to such breach shall be final and binding on the system integrator
2. In the event of the breach of any of the major and significant terms and conditions of this agreement by the system integrator, OCAC will give 60 days' notice to system integrator to cure the breach of the terms and conditions of the agreement then in that case System Integrator must cure within 60 days. In case the breach will continue till/after expiry of such cure period, OCAC will terminate the agreement.
3. Effects of Termination
4. Upon expiration or termination of this Agreement:

- a. The System integrator shall:
  - i. Notify forthwith the particulars of all project assets.
  - ii. Deliver forthwith actual or constructive possession of the assets free and clear of all encumbrances and execute such deeds, writings and documents as may be required for fully and effectively divesting the Bidder all of its rights, title and interest in the State Data Centre
  - iii. Deliver relevant records and reports pertaining to the State Data Centre and its design, engineering, operation, and maintenance including all operations & maintenance records and manuals pertaining thereto and complete as on the date of termination or expiration. And
  - iv. Shall expeditiously settle the accounts.
- b. In the event OCAC terminates this Agreement pursuant to any material breach by the System Integrator to complete its obligations under this Agreement, Performance Bank Guarantee furnished by SI may be forfeited for reasons, to be recorded in writing.
- c. Upon termination (or prior to expiry/ upon expiry, as the case may be) of this Agreement, the Parties will comply with the Exit Management Clause set out in this Agreement
- d. OCAC agrees to pay the System Integrator for all charges for Services / Equipment provided by it and accepted by OCAC till effective date of termination.
- e. Any and all payments under this clause shall be payable only after the System Integrator has complied with and completed the transition and exit management as per the Exit Management Clause approved by OCAC. In case of expiry of the Agreement, the last due payment shall be payable to the System Integrator after it has complied with and completed the transition and exit management as per the exit management clause. Approved by OCAC
- f. SI immediately upon termination, discontinue providing any or all of the services contemplated hereunder.
- g. OCAC shall upon termination, by under no obligation to make any payments to System Integrator forthwith, except for any payments that may be due and payable to SI in respect of satisfactory services already completed as per scope of this agreement; and
- h. SI shall return all the property which belongs to OCAC including any data, information, files of completed or unfinished work. SI shall have no lien over the property of OCAC.
- i. Upon the termination or expiration this agreement , in case before complete delivery of materials, then the title and ownership of all materials, plans, ideas, services or

information ( developed by System Integrator for OCAC ) shall be transferred by SI to OCAC. Thereafter, OCAC, shall have no liability to SI's service arising from OCAC's use of any material was approved ,used, published or presented by or on behalf of OCAC. SI shall transfer such property, and documentation related thereto, to OCAC immediately after termination in case termination happens before complete delivery of materials.

**Termination due to bankruptcy of the System Integrator** – OCAC shall serve a written notice on the System Integrator at any time to terminate this Agreement with immediate effect in the event that the System Integrator reporting an apprehension of bankruptcy to OCAC or its nominated agencies. No Charges to the system integrator shall be payable in case of termination under this clause except for the equipment satisfactorily delivered and approved by OCAC as per the terms of this Agreement and services performed by the System Integrator up to the date of termination.

#### 4.12. Consequences of Breach and penalties

In the event of breach, OCAC shall have the right to recover any loss, damage or cost of hardship caused due to the breach of the terms of this Agreement, from the payment due to the System Integrator notwithstanding the above, in the event the amount due to the System Integrator fall short of the costs incurred or suffered by OCAC on account of loss, damage or cost of hardship, the System Integrator shall also be liable to make good all such losses, damages or cost of hardship caused to OCAC.

#### 4.13. Statutory Compliances

- System Integrator shall comply with all applicable statutes. OCAC shall not be liable in any manner whatsoever for any non-compliance on part of the System Integrator of the applicable laws and in the event of any adverse claim of whatsoever nature arising thereof, the entire burden shall be strictly borne by the System Integrator.
- System Integrator shall maintain all requisite records, registers, account books etc. related to this project which are obligatory under any applicable law in connection with the Services being rendered or work being performed to OCAC and shall provide such information as may be required under any law to any authority.

#### 4.14. Consequences of Termination

1. In the event of termination of the Contract due to any cause whatsoever, whether consequent to the stipulated term of the Contract or otherwise, OCAC shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the

Service(s) which the Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/material breach, and further allow the next successor Vendor to take over the obligations of the erstwhile

2. Vendor in relation to the execution/continued execution of the scope of the Contract.
3. Nothing herein shall restrict the right of OCAC to invoke the Guarantee and other guarantees, securities furnished, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available OCAC under law or otherwise.
4. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.
5. Upon Termination of the Contract, the System Integrator shall:
  - Prepare and present a detailed exit plan within five calendar days of termination notice receipt to the customer.
  - The customer and along with designated team will review the Exit plan. If approved, SI shall start working on the same immediately. If the plan is rejected, SI shall prepare alternate plan within two calendar days. If the second plan is also rejected, the customer or the authorized person will provide a plan for SI and it should be adhered by in totality

#### 4.15. Indemnification

Successful System Integrator hereby indemnifies, hold harmless & undertakes to defend OCAC, its affiliates and their respective employees, officers and directors against any claim by a third party including but not limited to damages, costs, expenses as a result of such claim with regard to:

- the extent that the System Integrator provided to OCAC by System Integrator under this Agreement infringes any third party's intellectual property rights;
- taxes/charges/cess/levies (and interest or penalties assessed thereon) against OCAC that are obligations of System Integrator pursuant to this Agreement;
- any damages for bodily injury (including death) and damage to real property and tangible personal property caused by the System Integrator;
- any claim or action by or on behalf of the System Integrator personnel based on his or her employment with the System Integrator, including claims arising under occupational health and safety, worker's compensation, provident fund or other applicable laws or regulations;
- claims by government regulators or agencies for fines, penalties, sanctions or other remedies arising from or in connection with the System Integrator failure to comply with its regulatory/legal requirements and compliances;

- any claim on account of an alleged breach of confidentiality and security of data occurring as a result of acts of omissions or commission of the System Integrator employees or sub-contractors;
- any claim occurring on account of misconduct, negligence or wrongful acts of omission and commission of employees of the System Integrator, and/or its sub-contractors;
- any claim occurring on account of misuse or negligent application, misuse of systems, failure to follow established procedure by the System Integrator and/or sub-contractor's employees;
- System Integrator shall ensure compliance with all applicable laws, local and Central, including all labor laws like ESI, EPF, Minimum Wages Act, Odisha Shops & Establishments Act, Contract Labour (Regulation and abolition) Act 1970, Payment of Bonus Act etc. and shall keep First Part indemnified and harmless in case of any action for violation by Second Part of any of the applicable laws so long as this arrangement is in force. For all purposes the persons deployed will be employees of second part and they will have no relation whatsoever with First Part. Second Part shall be responsible to furnish all such information/documents to First Part in this regard as may be required by it from time to time. Furthermore, Second part shall be responsible to furnish self- attested copies of all returns/challans filed by second part in the office of ESI, EPF, Minimum Wages Act, Contract Labour etc. on monthly basis to the first party, in case, the second part fails to submit or not willing to submit the copies of returns, first part shall be entitle to stop the payments till the submissions of the returns.
- In event of any theft, loss, damage, destruction, or any other act of vandalism or sabotage of the property of the Customer in the possession of the System Integrator by virtue of this agreement, the System Integrator shall be liable to indemnify the first part to the extent of damage or loss so caused.
- System Integrator has all the requisite consents, licenses and permissions to (I) enter into this Agreement (ii) carry out the obligations set out in this Agreement and it shall keep all such consents, licenses and permissions renewed and valid at all times during the continuance of the Agreement.

#### 4.16. Limitation of Liability

- Neither Party; nor its subsidiaries or its affiliates will be liable to the other Party, whether in contract, or (including negligence), strict liability or otherwise, for loss of business, revenue, profits, loss of goodwill or reputation; or indirect, consequential, or special loss, arising in connection with any order, product, service, related documentation, information and/or the intended use thereof, even if a Party has been advised, knew or should have known of the possibility of such damages.



- Subject to the above and notwithstanding anything to the contrary elsewhere contained herein, the maximum aggregate liability of the bidder for all claims under or in relation to this agreement shall be regardless of the form of claims shall be limited to 100% of the amount to be paid to SI by OCAC under the applicable statement of work that gives rise to such liability (as of the date the liability arose).

#### 4.17. Dispute Resolution and Arbitration

##### I. Dispute Resolution

- OCAC and the System Integrator shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with this Agreement. All negotiations, statements and/or documentation pursuant to these disputed matter shall be without prejudice and confidential (unless mutually agreed otherwise). The time and resources costs of complying with its obligations under this provision shall be borne by respective Parties. All Arbitration proceedings shall be held at Bhubaneswar, Odisha, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.
- On non-settlement of the dispute, same shall be referred to the Commissioner-cum-Secretary to Government, E&IT Department, Government of Odisha for his decision and the same shall be binding on all parties, unless either party makes a reference to arbitration proceedings, within sixty days of such decision.

##### II. Arbitration

- Any and all disputes, controversies and conflicts ("Disputes") arising out of this Agreement between the Parties or arising out of or relating to or in connection with this Agreement or the performance or non-performance of the rights and obligations set forth herein or the breach, termination, invalidity or interpretation thereof shall be referred for arbitration in terms of the Arbitration and Conciliation Act, 1996 or any amendments thereof. Prior to submitting the Disputes to arbitration the Parties shall resolve to settle the Dispute/s through mutual negotiation and discussions. In the event that the said Dispute/s are not settled within thirty ( 30) days of the arising thereof ,the same shall finally be settled and determined by arbitration in accordance with the Arbitration & Conciliation Act ,1996 or any amendment thereof .The place of arbitration shall be Bhubaneswar and the language used in the arbitral proceedings shall be English .
- The arbitral award shall be in writing and shall be final and binding on each Party and shall be enforceable in any court of competent jurisdiction. None of the Parties shall be entitled to commence or maintain any action in a court of law upon any Dispute

arising out of or relating to or in connection with this Agreement ( infringement of IPR Excepted ) ,except for the enforcement of an arbitral award or as permitted under the Arbitration & Conciliation Act ,1996 .

#### 4.18. Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the SI or OCAC as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:

- Neither Party shall be responsible to the other for any delay or failure in performance of its obligations due to any occurrence commonly known as Force Majeure which is beyond the control of any parties, including, but is not limited to, flood, explosion, thundering, acts of God or any Governmental body, public disorder, riots, embargoes, or strikes, acts of military authority, epidemics, lockouts or other labour disputes, insurrections, civil commotion, war, enemy actions.
- If a Force Majeure arises, the System Integrator shall notify promptly within a reasonable time frame to OCAC in writing of such condition and the cause thereof. Unless otherwise directed by OCAC, System Integrator shall continue to perform his obligations under the Agreement as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- The System Integrator shall be excused from performance of his obligations in whole or part as long as such cases, circumstances or events shall continue to prevent or delay such performance. Neither Party shall have any liability to the other Party in respect of the termination of this Agreement as a result of an event of Force Majeure.
- In case of a Force Majeure, all Parties will endeavor to agree on an alternate mode of Performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure.
- System Integrator shall be paid for supply and services till last date of termination in case of force majeure
- If force majeure conditions continue for more than 30 days and the services are suspended then either party has the right to terminate this agreement.

#### 4.19. Confidentiality

- OCAC may allow the System Integrator to utilize Confidential Information and the System Integrator shall maintain the highest level of secrecy, confidentiality and privacy with regard to such Confidential Information. The System Integrator shall use

its best efforts to protect the confidentiality and proprietary of Confidential Information.

- Additionally, the System Integrator shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities. The System Integrator shall use the information only to execute the Project.
- OCAC shall retain all rights to prevent, stop and if required take the necessary punitive action against the System Integrator regarding any forbidden disclosure.
- The System Integrator may share the confidential information with its employees, affiliates, agents and subcontractors but only strictly on a need to know basis in order to accomplish the scope of services under this Agreement. Upon request of OCAC, the System Integrator shall execute a corporate non-disclosure agreement (NDA) with OCAC in the mutually agreed format provided by OCAC shall ensure that all its employees, agents and sub-contractors are governed by confidential obligations similar to the one contained herein. The SI and its antecedents shall be bound by the NDA. The SI will be held responsible for any breach of the NDA by its antecedents/ delegates/ employee/ subcontractors etc.
- To the extent the System Integrator shares its confidential or proprietary information with OCAC for effective performance of the Services, the provisions of the confidentiality Clause (I) to (iii) shall apply mutatis mutandis on OCAC.
- The Bidder shall not use Confidential Information, the name or the logo of the OCAC except for the purposes of providing the Service as specified under this contract;

#### 4.20. Fraud and Corrupt practices

- The SI and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the Selection Process. For this purpose the definition of corrupt and fraudulent practices will follow the provisions of the relevant laws in force. Notwithstanding anything to the contrary contained in this RFP, OCAC shall reject a Proposal without being liable in any manner whatsoever to the SI, if it determines that the SI has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the "Prohibited Practices") in the Selection Process. In such an event, OCAC shall, without prejudice to its any other rights or remedies, declare the SI ineligible, either indefinitely or for a stated period of time, forfeit and appropriate the Proposal Security or Performance Security, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to the

Authority for, inter alia, time, cost and effort of the Authority, in regard to the RFP, including consideration and evaluation of such SI Proposal.

- Without prejudice to the rights of OCAC under Clause above and the rights and remedies which OCAC may have under the LoI or the Contract Agreement, if an SI or Systems Integrator, as the case may be, is found by OCAC to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the LoI or the execution of the Agreement, such SI shall not be eligible to participate in any RFP or RFP issued by OCAC during a period of < period, suggested 2 (two) > years from the date such SI, as the case may be, is found by OCAC to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.
- For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:
  - a) "Corrupt practice" means Engaging in any manner whatsoever, whether during the Selection Process or after the issue of the LoI or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the LoI or the Agreement, who at any time has been or is a legal, financial or technical consultant/ adviser of OCAC in relation to any matter concerning the Project;
  - b) "fraudulent practice" means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process; the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of OCAC who is or has been associated in any manner, directly or indirectly with the Selection Process or the LoA or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of OCAC, shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or
  - c) "Coercive practice" means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person's participation or action in the Selection Process;

- “Undesirable practice” means establishing contact with any person connected with or employed or engaged by OCAC with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or having a Conflict of Interest; and
- “Restrictive practice” means forming a cartel or arriving at any understanding or arrangement among SIs with the objective of restricting or manipulating a full and fair competition in the Selection Process.

#### 4.21. Exit Management Plan

The SI shall not exit from the contract within stipulated time period of five (5) years after Go-Live. However, in the event that the SI decides to opt out of the contract prematurely it has to notify the authority six months in advance through a written letter, SI will not seek ownership rights over the equipment and its PBG will also be forfeited.

If the SI exits from the contract during the execution within the stipulated time period then OCAC reserves the right to terminate the contract and may ask the bidder with L2 price to match the price of L1 and execute the remaining work as per RFP scope of work.

The SI shall document and submit a detailed Exit Management Plan (EMP) at OCAC for approval within 90 days post signing of the contract. The Exit Management Plan shall be re-drafted/ reviewed by SI in annual basis and need to be submitted to OCAC.

##### **I. Purpose of Exit Management Plan**

- a) This clause sets out the provisions which will apply upon completion of the contract period or upon termination of the agreement for default of the System Integrator. The Parties shall ensure that their respective associated entities, in case of OCAC, any PMU/Agency appointed by OCAC and in case of the System Integrator, the sub-contractors, carry out their respective obligations set out in this Exit Management Clause. Exit Management criteria will be a part of Master Service Agreement with detailed information about exit criteria and exit management plan.
- b) The exit management period starts, exactly period of 30 days before, in case of expiry of contract, or on the date when the contract comes to an end and up to period of 30 days in case of termination of contract, or on the date when the notice of termination is sent to the System Integrator. The exit management period ends on the date agreed upon by OCAC or one year after the beginning of the exit management period, whichever is earlier.
- c) The System Integrator shall divest all the project assets at the beginning of the Exit management period to OCAC at zero value in case of expiry of contract and at the depreciated rate as per Indian Income Tax Act if there is a termination of contract.

- d) The System Integrator shall pay all transfer costs and stamp duty applicable on transfer of project assets except in case the Project is being terminated due to default of OCAC, where OCAC shall be responsible for transfer costs and stamp duty, if any. For clarification of doubt, transfer costs in this Clause relate to taxes and duties applicable due to transfer of the OSDC 2.0 project, if any.

At the beginning of the exit management period, the System Integrator shall ensure that

- i. All Project Assets including the hardware, software, documentation and any other infrastructure shall have been cured of all defects and deficiencies as necessary so that the OSDC 2.0 Project is compliant with the Specifications and Standards set forth in the RFP, Agreement and any other amendments made during the contract period;
- ii. The System Integrator delivers relevant records and reports pertaining to the OSDC 2.0 Project and its design, engineering, operation, and maintenance including all operation and maintenance records and manuals pertaining thereto and complete as on the Divestment Date;
- iii. On request by OCAC , or any PMU/Agency appointed by OCAC, the System Integrator shall effect such assignments, transfers, licenses and sub-licenses related to any equipment lease, maintenance or service provision agreement between System Integrator and any PMU/Agency, in favour of OCAC, or any PMU/Agency appointed by OCAC, if it is required by OCAC, or any PMU/Agency appointed by OCAC, and is reasonably necessary for the continuation of services by OCAC, or any PMU/Agency appointed by OCAC;
- iv. The System Integrator complies with all other requirements as may be prescribed under Applicable Laws to complete the divestment and assignment of all the rights, title and interest of the System Integrator in the OSDC 2.0 Project free from all encumbrances absolutely and free of any charge or tax to OCAC or its nominee.

## **II. During the Exit Management period**

- i. The System Integrator will allow OCAC, GoO or any third party appointed by OCAC, GoO, access to information reasonably required to define the then current mode of

operation associated with the provision of the services to enable OCAC, GoO or any PMU/Agency appointed by OCAC, GoO to assess the existing services being delivered;

- ii. Promptly on reasonable request by OCAC, GoO or any PMU/Agency appointed by OCAC, GoO, the System Integrator shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with the "Contract", the Project Plan, SLA and scope of work, relating to any material aspect of the services (whether provided by the State Data Centre 2.0 System Integrator or sub-contractors appointed by the System Integrator). OCAC, GoO or any PMU/Agency appointed shall be entitled to copy all such information. Such information shall include details pertaining to the services rendered and other performance data. The System Integrator shall permit OCAC, GoO or any PMU/Agency appointed to have reasonable access to its employees and facilities as reasonably required by OCAC, GoO or any PMU/Agency appointed to understand the methods of delivery of the services employed by the System Integrator and to assist appropriate knowledge transfer.
- iii. Before the end of exit management period, the System Integrator will assist in a successful trial run of Network administration, Facility management including helpdesk management by OCAC, GoO or by any PMU/Agency appointed.

### **III. Hand Over of Assets/ Documents**

- i. SI shall handover the peaceful possession of Project Assets in good and working condition with detail list showing the name of the equipment and with configuration to the Purchaser/replacement SI as authorized by Purchaser customer within 30 days of the date of serving of notice or within the Transition Period.
- ii. The SI shall provide all such information available with it during the contract execution or during the Operation & management phase as may reasonably be necessary within a reasonable period not exceeding 30 days of the date of serving of notice or within the Transition Period.
- iii. Existing SI will hand over the documents to OCAC or new SI, pertaining to the operation of OSDC i.e. all configuration records, purchase orders, installation reports, FAT/PAT records, SLA records, SLA methodology, SLA calculation template, MIS reports, ISO documents (procedures, records, templates, standards), Audit records, security assessment and risk records, all SOPs, warranty documents, AMC documents, Knowledge documents (KEDB), Training records etc.

#### 4.22. Severability and Waiver

If any provision of this Agreement, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the remainder of the provisions in question which shall remain in full force and effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid or unenforceable provision by a valid and enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the illegal, invalid or unenforceable provision or part provision. No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement of any right, remedy or provision of this Agreement shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of such right, remedy or provision or the exercise or enforcement of any other right, remedy or provision.

#### 4.23. Applicability of Liquidated Damages

The System Integrator shall accomplish the scope of work under this Agreement as per the Project Timelines and as per the Service Level Agreements. If the System Integrator fails to achieve the Project Timelines or if it fails to achieve the Service Levels (in the SLAs) for any reason whatsoever, the System Integrator shall be liable to pay liquidated damages as provided in **QGR SLA and Penalty Table & LD Table** of this Agreement. OCAC shall have the right to determine such extent of fault and liquidated damages in consultation with System Integrator and any other Party as it deems fit. Payment of liquidated damages shall be the sole and exclusive remedies available to OCAC. Liquidated damages will be 1 % of the Capex cost for delay of every week and capped at 10% of the cost of Capex as mentioned in the Agreement.

If the liquidated damages exceeds the cap as mentioned in the Agreement, the Purchaser or OCAC shall have the right to terminate the agreement for default and consequences for such termination as provided in the agreement shall be applicable. In case it leads to termination, OCAC shall give Sixty days' notice to the SI of its intention to terminate the contract and shall so terminate the contract unless during the Sixty days' notice period, the SI initiates remedial action acceptable to OCAC.

Each of the Parties shall ensure that the range of the Services/Deliverables under the SLA shall not be varied, reduced or increased except with the prior written agreement /consent between the Purchaser and the SI in accordance with the provisions of change request procedure as set out in this Agreement.



If the Goods and Related Services supplied do not meet the minimum specifications as per the Contract, and the same is not replaced/modified by the SI to meet the requirements within 14 days of being informed by the OCAC, the OCAC shall be free to impose any penalty as deemed fit. In addition, the OCAC shall reserve the right to terminate the contract and recover liquidated damages by forfeiting the performance bank guarantee submitted by the SI.

#### 4.24. Intellectual Property Rights

- All Intellectual Property of OCAC under the Letter of Invitation and/ or the Contract will belong exclusively to GoO, except the pre-existing intellectual property rights of the Bidder, its subcontractors (if any). On payment of all of consultant's fees in connection with this Agreement and subject to the other provisions of this Agreement, GoO shall at all times retain to use within its internal business all right title and interest in and to any Intellectual Property Rights in the deliverables to be provided by the Bidder under this Agreement and any modifications thereto or works derived from there except the pre-existing intellectual property rights of Consultant or its subcontractors (if any, and Consultant Technology. It is hereby expressly clarified that Bidder shall have no right, title or interest in or to such Intellectual Property Rights of OCAC for any purpose, except the right to use, modify, enhance and operate such designs, programs, modifications as per requirement of OCAC. Bidder shall not use such Intellectual Property of OCAC for any other purpose during and after the term of the Contract.
- No services covered under the Contract shall be sold or disposed by the Bidder to OCAC in violation of any right whatsoever of third party, and in particular, but without prejudice to the generality of the foregoing, of any patent right, trademark or similar right, or any charge mortgage or lien.
- Subject to clause (c) below, the Intellectual Property Rights of all the database, programs, reports, formats etc. developed/created for this project would be of OCAC / GoO.
- The Bidder shall continue to retain sole ownership of the pre-existing proprietary knowledge, tools, source code, records, SOPs, application configurations, drawings, methodology, templates, works of authorship, materials, information plus any modifications or enhancements thereto and intellectual property content brought in by Bidder to this engagement and/or incorporated in the deliverables submitted by Bidder to OCAC or created independently of the performance of the Services ("Consultant Technology"). For avoidance of doubt, it is clarified that Consultant or its subcontractor shall have the right to use any works of authorship or other intellectual property that may be included in the Deliverables, to develop for themselves, or for others, materials or processes that may be similar to those produced as a result of the Services. Further,

any third party licenses other than the hardware and software to be used by the Bidder resources for delivering the deliverables under this Agreement, necessary for the performance of the Services under this Agreement, would need to be procured by OCAC. Bidder hereby undertakes;

- Not to provide access to the Intellectual Property of OCAC to persons other than authorized users to ensure that all authorized users are appropriately notified of the importance of respecting the Intellectual Property Rights of OCAC and that they are made aware of and undertake to abide by the similar terms and conditions of the this Agreement. Not to permit any person, other than the authorized users, to copy, duplicate, translate into any language, or in any way reproduce the Intellectual Property of OCAC. To effect and maintain reasonable security measures to safeguard the Intellectual Property of OCAC from unauthorized access or use by any third party other than the authorized users. To notify OCAC promptly of any unauthorized disclosure, use or copying of the Intellectual Property of OCAC of which Bidder becomes aware. To change the manpower deployed if OCAC notifies issue (along with the justifiable ground) in the satisfactory performance of the respective resource.
- The SI shall retain exclusive ownership of all methods, concepts, algorithms, trade secrets, software documentation, other intellectual property or other information belonging to the SI that existed before the effective date of the contract.

#### Notices

Any queries or other document, which may be given by either Party under this Agreement or under the SLA, shall be given in writing in person or by pre-paid recorded delivery post or by facsimile transmission or through email to the notified address.

In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below:

- (i) To OCAC:  
Attention: General Manager (Admin)  
Odisha Computer Application Centre,  
N1/ 7D, Acharya Vihar Square, Near Planetarium,  
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013
- (ii) To  
[Name and Address of Successful Bidder]

Any notice or other document shall be deemed to have been given to the other Party (or,

if relevant, its relevant associated company) when delivered (if delivered in person) if delivered between the hours of 10.00 am and 5.00 pm on a working day at the address of the other Party set forth above or if sent by fax, provided the copy of the fax is accompanied by a confirmation of transmission, or on the next working day thereafter if delivered outside such hours, and 7 days from the date of posting (if by letter).

Notice can also be given through email address furnished by the System Integrator. The time of the sent message in outbox of the sender will be considered to be time of delivery of the message.

Either Party to this Agreement or to the SLA may change its address, telephone number, facsimile number and nominated email for notification purposes by giving the other reasonable prior written notice of the new information and its effective date.

#### 4.25. Taxes and Duties

All payments will be subjected to tax deduction at source as applicable/ required at the prevailing tax rates. Any changes, revision or enactment in duties like GST, taxes or any CESS during the period of validity of the Bids and also during the contract period by Central/State/Other Government bodies will be considered and applied after due consideration. The decision of OCAC in this regard will be final and binding and no dispute will be entertain. Any taxes at the time of supply goods and services shall be applicable as per the Law.

For goods supplied from outside the Purchaser's country, the SI shall be entirely responsible for all applicable taxes, license fees, and other such levies imposed outside the Purchaser's country. The basic price quoted item wise by the bidder in respect of the transaction between OCAC & the SI shall include all taxes & duties and charges payable by the bidder except for the GST, CGST plus OGST, or IGST, as the case may be, at applicable rate shall be quoted alongside the basic price for all the items. However, while quoting the basic price against the package/works, benefit of Input Tax Credit (ITC) should be adjusted in the quoted price by the SI.

#### 4.26. Insurance

Appropriate insurance to cover all solution components for the transit period and until the time of its acceptance at the respective site is to be taken by the SI. As the SI will carry the risk for the material in his books during transit, the SI should arrange insurance for the total system as period from the dispatch till Acceptance Test is successfully achieved. Further the SI is to take all required insurance coverage in respect of all its personnel who shall be working on this engagement.

#### 4.27. Audit, Access and Reporting

The System Integrator shall allow access to or its nominated agencies to restricted to all data related to OSDC 2.0 which is in the possession or control of the System Integrator or its subcontractors, agents, suppliers etc. and which relates to the provision of the Services as set out in the Audit, Access and Reporting Schedule and which is reasonably required by OCAC to comply with the terms of the Audit, Access and Reporting of this Agreement.

OCAC would also conduct audit of the process, plan and results of the Acceptance Test carried out by the System Integrator. OCAC shall verify availability of all the defined services as per the contract signed between the SI and OCAC. The SI shall be required to demonstrate all the services / features / functionalities as mentioned in the agreement.

#### 4.28. Ownership

- Products and fixes: all COTS (Commercial off-the-shelf) products and related solutions and fixes provided pursuant to this Agreement shall be licensed according to the terms of the license agreement packaged with or otherwise applicable to such product. The System Integrator would be responsible for arranging any licenses associated with products. "Product" means any computer code, web-based services, or materials comprising commercially released, pre-release or beta products (whether licensed for a fee or no charge) and any derivatives of the foregoing which are made available to OCAC for license which is published by product owner or its affiliates, or a third party. "Fixes" means product fixes that are either released generally (such as commercial product service packs) or that are provided to OCAC when performing services (such as workarounds, patches, bug fixes, beta fixes and beta builds) and any derivatives of the foregoing. All intellectual property rights in any exclusive development to meet the functional requirement of this Agreement shall be owned by OCAC.
- Training and other material: The ownership of all IPR rights in any and all documents, artefacts, etc. (including all training material) made pursuant to this Agreement during the Term for implementation of the Project under this Agreement will lie with OCAC.

#### 4.29. Safety Regulations

- Successful Bidder shall be responsible to take all precautions to ensure the safety of the person or property of the OCAC and Data Centre while performing its obligations hereunder

- It is the responsibility of the bidder to carry the material/equipment to the location of the installation; SI will be penalized for any damage caused to property/ OCAC Tower building.
- It is the responsibility of the Successful Bidder to comply with all sorts of safety measures under applicable law in regards to men and material deployed for the project.

#### 4.30. Warranty of Equipment

- The Bidder is required to provide warranty valid for Five (5) Years, for all supplied equipment as per financial bid format provided in the RFP. All Products supplied under the RFP should not reach end of support before 7 years from the date of FAT or start of O & M services. All the IT / Non- IT products quoted should be supported by the SI for next 5 years from the start date of O & M services. The SI should also commit support for another 2 years if necessary.
- The Bidder shall warrant that all the equipment supplied under the contract is newly manufactured and shall have no defect arising out of design, materials or workmanship or from any act or omission of the Bidder that may develop under normal use of the supplied equipment's in the conditions prevailing across the country.
- The Bidder shall warrant that the services provided under the contract shall be as per the Service Level Agreement (SLA) defined in the tender.
- This warranty, for all equipment's, shall remain valid for Five (5) Years after the complete installation and final commissioning & Go –Live of the Data Centre. The installation will be deemed incomplete if any component of the equipment or any documentation/media is not delivered or is delivered and not installed and/or not operational or not acceptable to OCAC after final acceptance testing.
- OCAC shall promptly notify the Bidder about any claims arising under this warranty. Upon receipt of such notice, the bidder shall repair/ replace/ reconfigure/ re-provision the defective equipment or service.
- The supplier shall ensure during the comprehensive warranty period that all the supplied stores continue to function as per the parameters mentioned in technical specification. During warranty period, maintenance of all stores including pick-up of the faulty equipment for repair, replacement and repair/fault rectification, delivery of

the rectified equipment shall be undertaken by the supplier at no additional cost to the buyer. The supplier will be responsible for the maintenance/preventive maintenance of the complete system. Any Malfunctioning or defective items shall be replaced by the supplier free of cost at project site as early as possible, under the following condition:-

- If the bidder, having been notified, fails to remedy the defect(s) within the period specified in the SLA, OCAC may proceed to take such remedial action as may be necessary at the Bidder's risk and expense and without prejudice to any other rights, which OCAC may have against the Bidder under the contract.
- All the software's used for providing data Centre services shall be licensed to OCAC and will be the property of OCAC.
- The SI shall be responsible for end-to-end implementation and shall quote and provide/supply any items not included in the bill of material but required for commissioning of the cloud, network, Non-IT equipment like PAC, UPS, BMS, EMS, Infrastructure Monitoring, including any Compute equipment. OCAC shall not pay for any such items, which have not been quoted by the SI in the bid but are required for successful completion of the project.

#### 4.31. OEM Certificate of Equipment

- The OEM Certificate as per the Proforma- 12, 13 & 14 as applicable stating that the bidding company is the Original Equipment Manufacturer of the equipment they are offering, shall produce signed declaration certificates, giving reference of this Tender Enquiry, who is authorized to offer their equipment and a commitment to provide maintenance support during the comprehensive warranty period.
- In case the stores are supplied by the authorized supplier of the OEM, then the OEM certificate (Proforma-12 & 13) shall state that, in case the authorized supplier fails to repair/ maintenance the equipment during the comprehensive warranty, the responsibility for maintenance of the equipment provided would then be taken over by the OEM.
- The complete contact details of the OEM (Name and designation of contact person, postal address, e mail ID and telephone & FAX numbers) will be furnished and the buyer may at his discretion verify the authorization from the OEM, failure of which may result in the bidder being black listed and / or barred from participating for any future tender of this organization.

#### 4.32. Comprehensive AMC of Equipment

- It is the responsibility of the selected bidder to operate and maintain OSDC for the entire contract period and shall bear all the recurring expenditure (AMC of the support equipment, Operating staff salaries, and Incidental expenses etc.) and bear any other expenses which are not covered under above for implementation of this project.
- It is the responsibility of the selected bidder to ensure AMC for the support equipment from time to time to keep the equipment in working condition during the contract period and shall bear this expenditure. However, consumables may be reimbursed as per actuals post approval from OCAC.

#### 4.33. Spares and Performance of Equipment

- The Bidder shall specify in the Technical Proposal the complete list of spares that will be maintained for meeting the various SLA parameters specified in the tender.
- The Successful Bidder shall stand guarantee for the supply of spares of all the equipment under the scope of supply for a minimum period of 5 years from the date of awarding the contract and also guarantee that discontinuity of production of any item offered as a part of the system shall not affect the maintainability of the system for a period of 5 years from the start date of operation and maintenance support of data Centre.

#### 4.34. Change Order and Contract Amendment

- OCAC may at any time order the selected bidder through Notice in accordance with clause "Notices" above, to make changes within the general scope of the Contract in any one or more of the following: - a. drawings, designs, or specifications, where Goods to be furnished under the Contract are to be specifically manufactured for the Purchaser; b. the place of delivery; and c. the related services to be provided by the selected bidder.
- If any such change causes an increase or decrease in the cost of, or the time required for, the selected bidder's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or in the Delivery and Completion Schedule, or both, and the Contract shall accordingly be amended. Any claims by the selected bidder for adjustment under this clause must be asserted within thirty (30) days from the date of the selected bidder's receipt of the Purchaser's change order.

- Prices to be charged by the selected bidder for any related services that might be needed but which were not included in the Contract shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the selected bidder for similar services.



## 5. Design Consideration for OSDC 2.0 (Non-IT)

Odisha State Data Centre 2.0 design and solution is completely Bidder/MSI's responsibility in this project. However, while doing so, the bidder must take into account the considerations/assumptions/suggestions as mentioned in this document. In case there is any discrepancy or contradiction, the same may be brought to the notice of the purchaser during pre-bid meeting only.

Design considerations are divided into following sections.

1. Space Allocation
2. General Design Requirements
3. Technical, Functional And Operational Requirements

### **SPACE ALLOCATION**

Described below is the minimum requirement of Rooms/ Enclosures in the Facility. Bidder must take these considerations while designing and planning.

#### 5.1. Civil/ Non- IT Design Consideration

The proposed Data Centre area shall be located at OCAC Campus, Bhubaneswar. (Images are for representational purpose only):

#### **(Proposed indicative Layout for 88 Nos of Racks)**

RFP – Extension of Odisha State Data Centre – OSDC 2.0

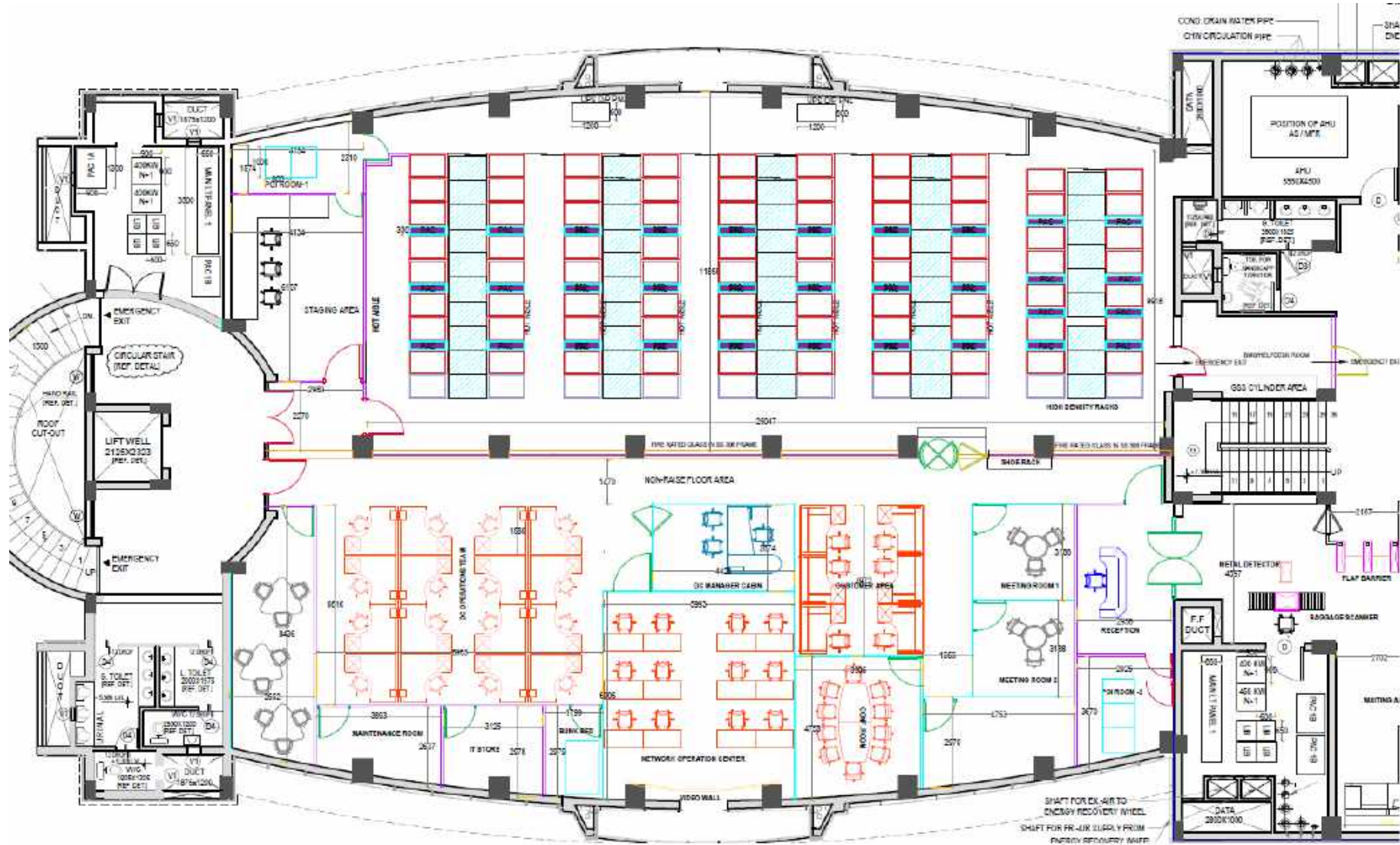


Fig. No-1

## 5.2. Data Centre Build/Non IT Design Consideration

1. The following are general design requirements. The requirements are not limited to the following and the best practices and standards prevalent for Data Centre has to be adhered while designing. The project is 'Turn-key' type in true sense. The successful bidder has to execute the project with accordance to the detailed scope as mentioned in the RFP.
2. The scope includes the supply, installation & commissioning of any material or equipment including civil works that are not specifically mentioned in the specifications and design details but are required for successful commissioning of the project.
3. The solution shall comprise of supply, installation, testing, commissioning training and handing over of all materials, equipment, hardware, software, appliances and necessary labor to commission said system complete with all the required components strictly as per ( but not limited to) the latest IS, IEC, IEEE, ASHRAE, NBC etc. codes.
4. The bidder shall provide detailed design, documentation, make, and model, efficiency including user, system and operation manuals along with the necessary diagrams, design drawings and details bifurcation of Bill of Quantity (BOQ) along with details description. The shop drawing ( to be submitted before execution or as on when required ) may include but not limited to the following
  - Site layout
  - Equipment placement layout
  - All drawing for Electrical scheme including single line diagram
  - All GA drawing of equipment
  - Piping schematic
  - Grounding and Earth pits
  - Lighting
  - Furniture placement
  - DG fuel pump
  - Complete HVAC system
  - Networking cabling
  - Trenches, cable trays and raceways
  - Shafts
  - Panel GA drawing
  - Fire detection and suppression system
  - Aspirating smoke detection, water leak detection, rodent repellent, CCTV, access control system
  - DCIM schematic

- Reflected ceiling plan
- Sectional views
- 3D drawing as required.

As and when required, the successful bidder has to submit the coordinated drawing for the solution.

5. The bidder shall be responsible for performing verification tests at their factory and at site to ensure all proposed software and hardware are functioning as per design at their own cost.
6. The bidder shall take the necessary clearance / approval of the drawings, design, quality of material, make and model of the quoted material etc. prior to the execution of the project

The server farm area load density will be as follows

- 80% of racks = 7.5 KW
- 20% of racks = 10 KW

### 5.3. Non IT Infrastructure (Scope of Work)

The minimum specified scope of work to be undertaken by the bidder for Design, Supply, Installation, testing, Commissioning, Operations and Maintenance of the proposed OSDC 2.0 at Bhubaneswar as per the scope mentioned below. The selected bidder shall ensure an uptime more than 99.982% on a quarterly basis for period of five years after Go Live.

The minimum specified work to be undertaken by the bidder for setting up and operating the proposed Data Centre OSDC 2.0, has been categorized as under:

- a. Develop appropriate design, make all required approval, Supply Installation Testing and commissioning including associated works of the proposed OSDC 2.0 at Bhubaneswar
- b. Data & Application migration from currently working State Data Centre to new Data Centre OSDC 2.0.
- c. Operations and Maintenance services for the complete Infrastructure at OSDC 2.0 at Bhubaneswar for the period of 5 years from the date of successful acceptance by OCAC.

*Note: The bidders are requested to submit their proposals for these Schedules in the same bid which would be combined for evaluation purposes.*

The scope shall comprise the design, supply, construction and testing of the proposed Data Centre building including all enabling works. All Works shall be carried out as per the proposed design and specifications and in accordance with the requirements of all relevant Indian standard codes.

The indicative scope of work (Area/Room wise) is illustrated below. Please note that the below descriptions are indicative in nature. The bidders should evaluate the site physically to understand the actual work requirement to complete the package before bidding for the same.

**Utility Room:**

The Utility room is between OCAC building and OCAC tower. This is a G+1 building. Following items are currently housed inside Ground floor of the building.

1. HT Panel
2. Transformers
3. Transformer output panel
4. ASLS panel ( Main LT panel)
5. Capacitor Panels
6. AMF panels for OCAC tower DG
7. Other small panels

The bidder is advised to do a detail site survey of the Utility room, take measurements and list out all the work required to revamp the room to make it better in terms of facility, manageability and operability.

The scope for the area are mentioned here but not limited to following.

1. The metering panel room is defunct and need to be taken up to make it functional. The bidder must inspect the metering panel room and propose revamp of the room to house two numbers of metering panel for two feeders. The door of the metering panel room must be with fire and water resistant material. It must also be noted that the rain water should not enter the metering panel room.
2. There are no walls on two side of the HT panel and Transformer area. The level of the floor is of the same level outside. To prevent water entering the area, a foot height brick wall with plaster needs to be constructed on both the side of the room.

The illustrative diagram is shown below for reference:

Illustrative diagram for Rolling Shutter:

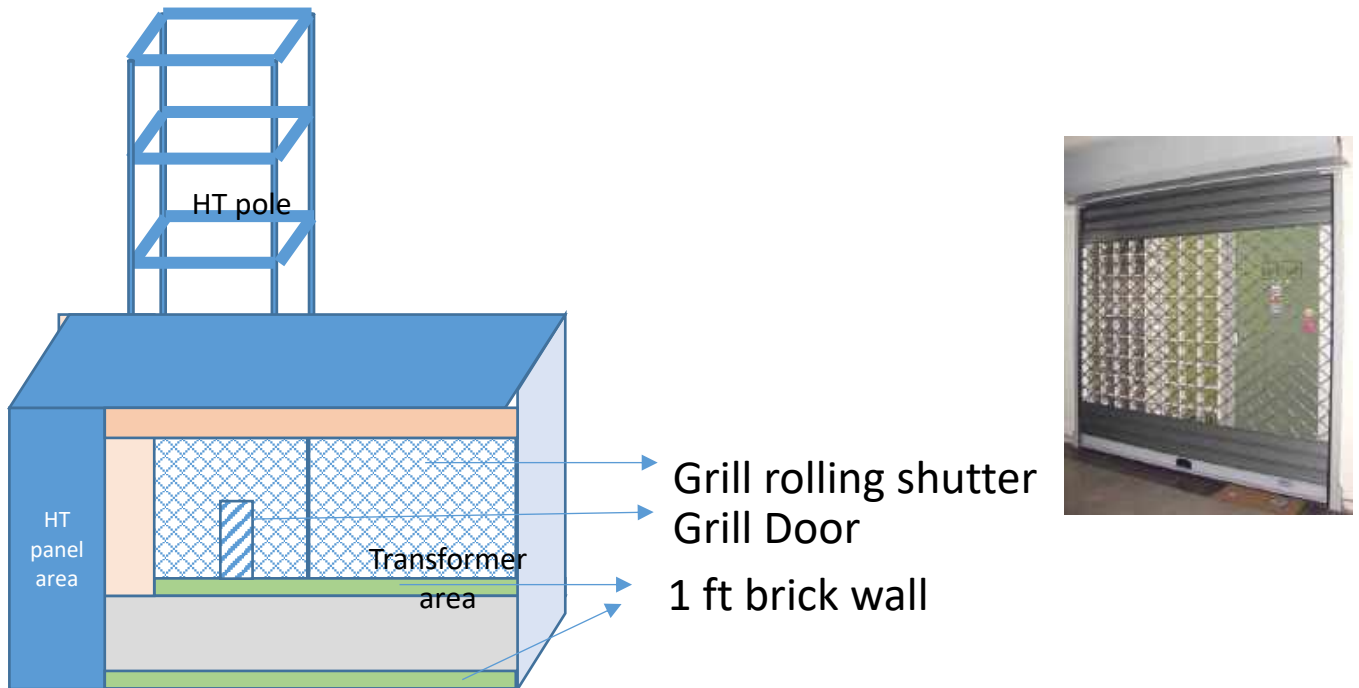


Fig. No-2

3. Transformer and HT panel housing room need to be closed from both the sides with grill rolling shutters with grill door as shown in the above illustrative figure. The shutter must have a 1200mm width and 2000 mm lockable door for entry and exit to the area.
4. The floor of the area need to be repaired with PCC after installation of HT panel and transformer. A layer of epoxy quoting must be done on the floor as a finishing layer.
5. The wall of the area needs to be painted with distemper.
6. Proper lighting arrangement to be done in the area. Lux level should be 250 measured at 1.5 meter from floor level at any point of the room. Only LED lights will be allowed.
7. The panel room in the building has many panels. Some of them are getting replaced with new one which are part of the scope of this RFP. All civil works required to be done in the process of panel replacement has to be done by the bidder.
8. The flooring has to be levelled and top layer to be epoxy quoted.
9. Currently the entry door is not available in the panel room. A door has to be created that has to be water and fireproof. Width of the door to be 2000 mm and height to be 2300 mm or the height available, whichever is maximum. The door can be double leaf door.
10. Exhaust fans to be installed in the panel room for 5 to 6 air changes in an hour.
11. Fire Extinguisher of minimum 4.5 Kgs suitable for such area to be provided in the rooms. One for Transformer area and 3 for panel room.

12. Dismantling existing Wall, Doors, Window or any structure of any material if required & removal of equipment such as panels, cables Debris from the site and storing, / disposing the same at a location as intimated by client will be in the bidder's scope.

**Campus Surroundings:**

- a. Existing trenches may be used for laying of cables. In the process, there may be chances of breakage of trench covers. The same has to be replaced by the Bidder with equal specification.
- b. The Existing DG set for the SDC area need to be replaced with new one. Accordingly the foundations for 2 Nos of DG set need to be created along with dismantling of existing roof shading & installation of fresh roof shading. It is expected that the 2 nos of Diesel Generators that is to be installed would be placed in a double tier Iron frame structure at a place as specified by OCAC. The bidder must submit a detail structural diagram with load bearing details of the structure before execution. The design has to be certified by a structural consultant.
- c. Cable Trenches: There are existing cable trenches available & may be used, however the bidder should evaluate & propose if there will be need to create new cable trenches. In case it is required the same may be proposed. In case trenches are required, the specification has to be same as existing one except the size of the trench.
- d. HSD Tank: Two no's of 5 KL underground HSD tanks need to be installed for 2 Nos of DG set for which suitable space to be identified & piping for the same should be done up to the DG sets. The DG fuel pipeline must have intrinsically safe Fuel meters with connectivity feature to DCIM. The meters must be integrated with DCIM tool. Each DG fuel consumption to be measured. Redundant pumps and piping to be installed as per Uptime Tier guidelines.
- e. Placement of Outdoor Area for PACs & CACs: It is proposed that AC ODUs on a platform of steel structure (using ISMB, ISMC of adequate size to cater the load) of 5 Meter height on the back side of the building adjacent to the 1<sup>st</sup> floor of the building (DC floor) level. The bidder should plan for the structure design accordingly. Bidder must submit a drawing and design for the platform duly authorized by a certified structural consultant.

**Data Centre Area (1st Floor of OCAC tower):**

- a. **Staircase & Ramp:** There are stair case & lift on both the sides for entry into Data Centre area.
- b. **Creation of Ramp:** There are needs of creation of 3 Nos of Ramps for smooth material entry inside the data center as per below:
  - i. Creation of Ramp with desired top finish from outside to building ground floor.
  - ii. Creation of Ramp with desired top finish from material entry side to server farm area.

- iii. Creation of Ramp with desired top finish from fire exit side of server farm area towards outside.
- c. There are three toilet blocks on each side of the Data Centre floor. One on the south side and two are on the north side. One of the blocks on the northeast side has to be converted to UPS and power room. All the partitions have to be dismantled & fittings/plumbing pipes to be removed & sealed. There has to be fire rated doors installed with minimum 1200 width for smooth entry of the equipment. The floor must be layered with antistatic material. The walls have to be painted with fire rated paint.
- d. The other side toilet block has to be furnished with high quality flooring, wall tiling and fixtures. Separate sections for MALE and FEMALE must be created. The scope includes floor and wall tile fittings, plumbing, Electrical, doors, windows, exhausts etc. All fittings inside the toilet to be approved by OCAC before installation. The toilet block has to be furnished with high quality flooring, wall tiling and fixtures. Bidder has to submit details of the toilet furnishing in a tabular form. The bidder needs to evaluate the same by site visits before quoting the prices.
- e. **Skirting:** Skirting need to be created whenever required.
- f. **Ceiling:** Server farm area will have no ceiling. However, a 23 mm nitrile rubber has to be pasted under the roof for thermal insulation. The workmanship should be such that it looks neat and clean without any tear, overlap, exposed roof, or non-aligned joints. The bidder must propose ceiling in the support area. However high quality modular mineral fiber ceiling with min 0.5 NRC may be accepted. Ceiling structure already existing near the lift area on both side has to be redone. The bidder may propose gypsum false ceiling wherever may require as per site demand.
- g. **Flooring:** Data Centre server farm area has to have raised floor of calcium sulphate material. The height must be 300mm from the floor. The floor tile UDL must be 1500 kg/Sq.Mtr and point load 450 KG.

Nitrile rubber Insulation 23 mm (minimum) under floor and true ceiling including skirting of desired specification must be laid in the server farm area for insulation.

Flooring for support area has to be with varieties of material such as, vitrified tiles, carpet tiles etc. The entry area from the north side (passenger lift side) must be highest quality double charged vitrified tile of 600x600 size.

All the power Rooms must be of antistatic PVC flooring of the required specification.

Initial PCC flooring may be required for the entire area before installations of vitrified tiles/carpet/epoxy/anti-static flooring. The same need to be evaluated by the bidders before bidding.



- h. **Partitions and walls:** A 230mm brick wall has to be constructed on one side (façade side) of the server farm. Light weight fly ash bricks must be used with cement mortar. The plaster must be with fine sand. A coat of putty and primer to be applied before the fire paint on the wall.
- i. The other side of the server farm wall must be fire rated glass of min 12 mm thickness. The height of the glass must be taken from +600 mm level till the false ceiling level of the corridor. Every glass will have a stainless-steel frame structure.
- j. The partitions in the Support area has to be mix of toughened glass (8mm min) or Gypsum board in UPVC frame. At least 70% of the walls in the support area should be of glass. The bidder should evaluate the requirements of Rooms as per indicative site layout & visit site before submission of bid in order to get the practical site feasibility.
- k. **Doors and Windows:** The doors requirement is given in the table below:

Sl. No	Door details	Type
01	Main entry door to facility from passenger lift side	Double leaf glass door of total 2000mm width
02	Entry to server room from corridor side	Fire rated glass door in UPVC frame
03	Entry to server farm from south side	Fire rated steel door (min 45mm thick and 1200 mm width) with vision glass
04	Entry to staging room	Fire rated steel door (min 45mm thick and 1200 mm width) with vision glass
05	Emergency exit from server farm to south side	Fire rated steel door of 45 mm thick and 900mm width
06	POE room entry	Fire rated door of 45 mm thick and 900mm width
07	Material Entry Door from material gate side	Fire rated steel door (min 45mm thick and 1200 mm width) with vision glass

<b>08</b>	Power room	Fire rated steel door (min 45mm thick and 1200 mm width) with vision glass
<b>09</b>	Toilets	900mm flush door
<b>10</b>	Support area	900mm toughened glass door and flush door wherever required

The above list is indicative only & the bidder may propose additional doors of desired specifications if required as per the actual site conditions.

There will be Designer privacy film on every glass Door.

- i. Bidder may decide to erect/not erect wall on the support area side east side as per requirement of their design. However, all the openings on the top and bottom of the gap between the glass façade and the building has to be closed with MDF board for ply board with smooth finish.
- m. **Paint and polish:** Server farm area walls, power room wall POI Rooms, Staging Area have to be mandatorily of fire rated paint. All other area must have premium emulsion paint of min 3 coats over and above putty and primer wherever required. All metallic exposure parts must be painted with Anti-Rust enamel Paint.
- n. **Furniture:** Furniture inside the support area is one of the most important aspects that must be looked at by the bidder. While selecting furniture, ergonomics, ease of maintenance, fire and moisture resistant properties and saving the environment aspect must be taken care of.

### **NOC Room Table/Desk/console:**

#### **Structure**

Console System must be of modular design. The Console design shall address the functional, ergonomic and aesthetic requirements of the particular working environment while complying with accepted human factor design and ergonomic standards for viewing distance, angle, keyboard, height, and knee space requirements.

- Standard top height of modular control desk shall be 750 mm. The Console Table Top / Working
- Surface should be made of 18mm MDF Board with 12mm Solid Acrylic Panel.
- The Basic Structure should consist of Extruded AL Profiles (6063T6 grade) binded by Top & Bottom (min 2mm) MS Frames formed in such a way as to provide maximum buckling and torsion resistance. The Front & Back Panels should be openable / removable (with Push Lock Mechanism) made of laminated MDF Board in min thickness of 18mm. The Side Panels should be fixed type, made in 26mm MDF Board Cladded on 18mm MDF Board. All panels must be attached to the frame with concealed fasteners. Console

access panels (Front & Rear Panels) must be removable without the use of tools. The Front panel should be positioned in such a way that there should be sufficient leg space (min of 400mm from the front edge of the Table Top).

- All sheet metal / aluminum parts must be finished with electrostatic powder coating with average of min 80 microns over all surfaces.
- The console frame shall have provisions for leveler legs to be incorporated into the frame.

### **Work Surface**

The Console Table Top should be made of 18mm MDF Board with 12mm Solid Acrylic Panel. The work surface platform shall have smooth edges and transitions, thus avoiding sharp corners or potential rib catchers for operator safety. Modular Rear Wall (Slat Wall) • Wall should be of min 86 mm (Height) and approx. 200-300 mm high from the Monitor Base. • Modular walls shall be made of 2mm thick Extruded Aluminium (6063T6 aluminium alloy). • It should have high Load bearing capacity. Minimum weight carrying capacity has to be 20 KGs per Meter.

### **Monitor Arms**

- It shall be capable for mounting all type of existing LCD monitor with dimensions between 19" to 27" using suitable adopter/additional base plate, if required any.
- Vendor shall provide the suitable adopter/additional base plate for mounting the existing LCD monitors. It shall allow the rotate/ tilt/ raise/the monitors as well as fix their adjustment.
- The monitor arm should be Articulating monitor arm.

### **Miscellaneous**

- There shall be a closed cabinet below the modular control desk for placing of CPU. Cabinet should have proper cooling system. CPU needs to be accessible from front as well as rear side of control desk for easy working and maintenance.
- The cabinet shutters shall be of Butt Hinged type with 18mm thick MDF.
- Rear shutters of each console should have provision of Airflow opening for cooling and heat dissipation effect.
- Rear panel shall have ventilation fans mounted on it.
- Hidden LED lights to be provided for Aesthetics.
- Adjustable Dimmable LED Light to be provided on the Desk.
- It shall have proper arrangement for flow of cables i.e. LAN Cable, Power cable, VGA cable, Mouse cable, Keyboard etc.
- Design of control desk shall allow cables from the floor cable channel.
- Control desk shall be equipped with individual power distribution unit (PDU) (06 no for one Modular Control Desk) and capable of being switched on/off individually. Power supply socket should be dual type i.e. Universal type.
- All bolts must be of SS material to avoid rust due to environment.

Bidder should submit the below certificates / documents after the completion of control desk / console: a) ANSI / BIFMA Certificate for Consoles

b) ISO 9001, ISO 14001 & OHSAS 18001 Certificate

c) Green Guard Certificate for low emissions

d) ROHS Compliance

e) ASTM E84



Fig. No-3

- o. **Cabin Desk/Table:** Each cabin will have a table for the officer who will use this for day to day work purpose. The selection of the table will be as per the following design, similar or better. The top surface must be made of MDF / Commercial board with laminate for a smooth finish. A side table with 3 drawers, a computer stand, bookshelf etc.



Fig. No-4

- p. **Office area Furniture:** Office area furniture should be modular type. An equivalent image is shown below. This bidder must select the furniture which has to be factory made as below, equivalent or better. All modular desks must have cable management system and raceways concealed inside the desk. Each seat must have 3 level drawer units.

- q. **Conference room table:** Conference room table must be for 14 seater with provisions for power and data outlets. An reference image of the table is given below. The top surface of the table must be water spill proof and smooth finish with matching laminate. The colour will be decided by OCAC prior to the delivery by the bidder.



Fig. No-5

- r. **Reception Table:** Reception table must be selected by allowing OCAC to make choices from from the available options by the bidder. The table must be for seating of 2 people with minimum size of 10ft x 3 ft. it must have provisions for power and data point with concealed cable management system. An reference image is givne as below. Korean table top finish is desired.



Fig. No-6

- s. **Breakout Canteen Furniture:** The break out and canteen furniture must be for minimum 15 people. Each table must be of size of seating of 3-4 people. Color and design must suite the overall ambience. A reference image is as given below.



Fig. No-7

- t. **Bunk bed:** A bunk bed is required for people who have to take rest on shift hours if required. A bed with mattress of soft leather finish must be installed in the bunk bed/ rest room. The bed has to be double layered made up of wood with smooth finish.

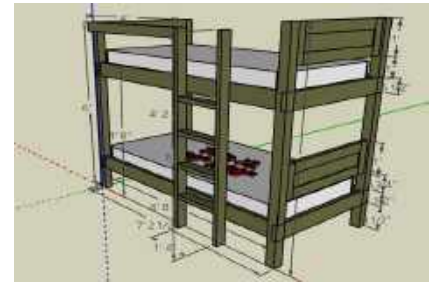


Fig. No-8

- u. **NOC room Chair:** NOC room chair must ergonomically designed in such a manner that long hour seating does not become tiring. The minimum requirement of chair is as follows.

Mid Back Chair  
Mesh Back & Silver Epoxy Backbone  
Synchronized Mechanism  
4-Way Adjustable Armrest  
Gas lift for Seat height adjustment  
Standard 5-prong P/Nylon Base  
BIFMA & GREEN GUARD certified

- v. **Conference Room Chair:** The conference room chairs are to be same as NOC room chair Except the BIFMA & GREEN GUARD certification.
- w. **Officer's chairs:** Same as the conference room chairs



Fig. No-9

- x. **Visitor's chair:** A reference image is given above. Bidder must select the chair as per this, equivalent or better.



Fig. No-10

- y. **Storage:** There has to be storage cabinets on all cabins, conference rooms, Bunk bed room, BMS room, Reception, Store room etc. All storage cabinets must be 2 ft depth and width as required. A reference image is given.



Fig. No-11

- z. **Shoe Rack:** A shoe rack must be supplied with 20 pair of slippers to be placed near the entrance of the server room. A reference image of the shoe rack is given below:



Fig. No-12

#### 5.4. Scope of Work – Electrical

##### **Electrical Design Concepts:**

The electrical design will be based on the Tier III design concept of Uptime Institute. The power flow from the source to load will pass through several stages of equipment.

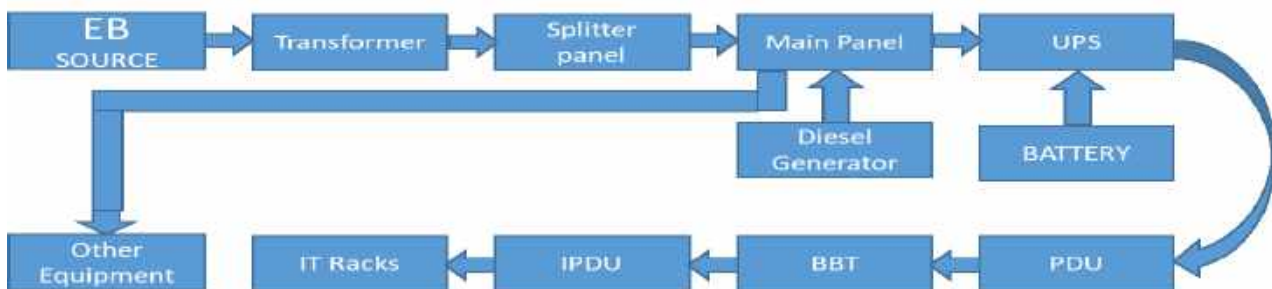


Fig. No-13

Redundancy and concurrent maintainability are important factors of the design. To achieve this dual path architecture must be adopted. The load details of the IT racks are as follows. Based on the load of IT equipment the entire system must be designed. The proposed design of the electrical scheme may be as follows.

**Existing scheme:**

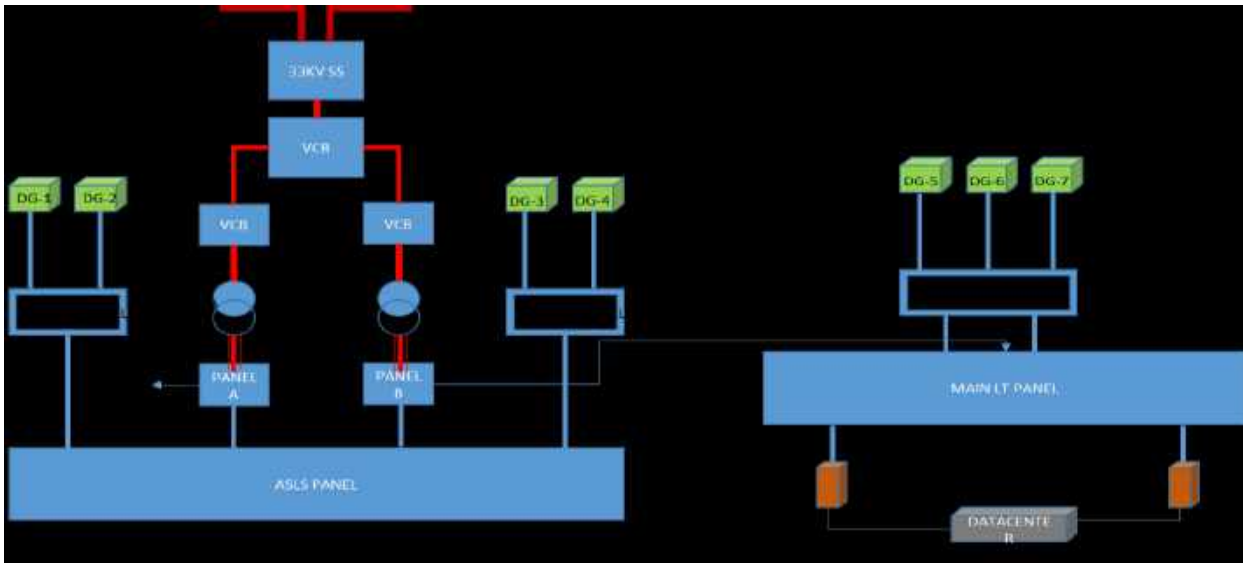
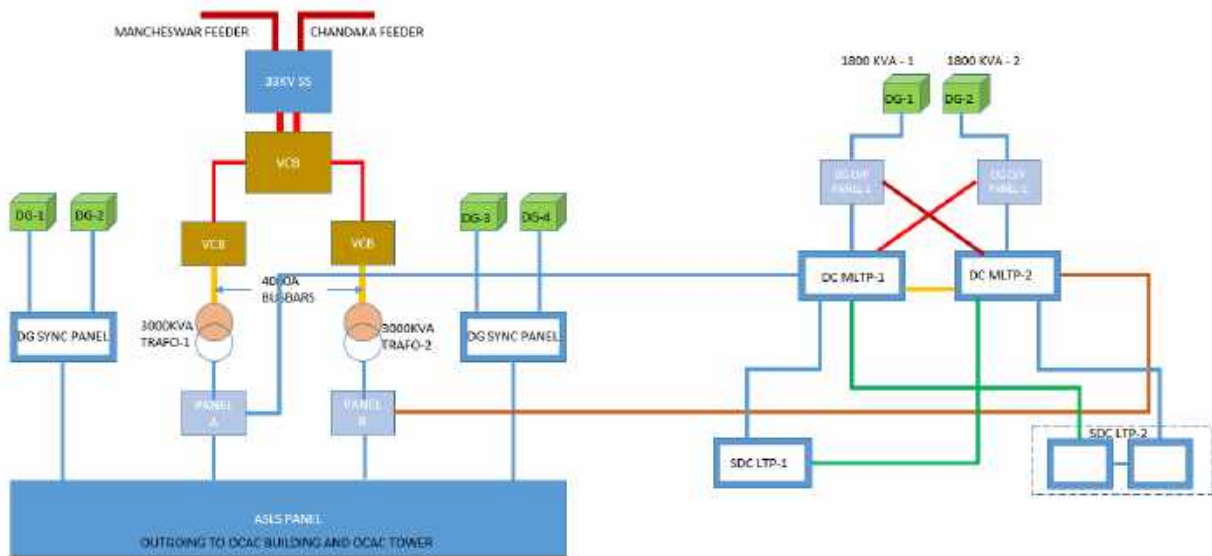


Fig. No-14

**Proposed Scheme:**



- # Metering panels to be installed for both feeders
- # VCB panels to be replaced with new one
- # HT cable will be replaced with new one
- # BBT will be replaced with Higher rating.
- # Transformer will be replaced with higher rating and type
- # Transformer output panel A & B will be replaced with new ones

- \* 2 nos 1800 KVA DG will replace 3 x 580 KVA at a suitable place
- \* DG sync panel will be removed as it will not be required.
- \* DC MLTP panel will new requirement and it will be placed in the Utility panel room
- \* Existing SDC -1 LT panel will continue to be there.
- \* SDC-2 LT panel will be installed in the Datacenter power room
- \* DG o/p panel A & B will be installed near DG area with IP 65 enclosure.

Fig. No-15



**Existing cable trenches:**

There are underground cable trenches running all around campus. The following length of trenches are available at site which can be used to run the proposed cables if feasible. However the bidder can propose new cable trenches if required.

Sl. No	From	To	Length	Width	Depth	Fill %
01	Utility Room	OCAC Tower	60 Meters	2.2 Meter	1.5 Meter	50 %
02	Utility Room	SDC-1 panel room	75 Meter	0.7 Meter	0.7 Meter	50 %
03	SDC DG area	DG sync panel room	12 Meter	0.8 Meter	0.8 Meter	50 %
04	HT cable entry point to campus wall	Utility room	50 Meter	0.8 Meter	0.8 Meter	50 %

The bidder should carefully evaluate the route of the cable /cable trenches and plan the new cable routes after visiting the site physically.

**Detail Scope Of Work (Illustrative SoW):****5.5. HT Power Distribution**

- i. There is a 33 KVA station inside the compound from where the two buildings OCAC and OCAC tower is powered. The HT panels need to be replaced with a new one with the same rating but with dual configuration. There are two feeders, one from Chandaka substation & another from Mancheswar substation is available.  
Currently one HT feeder is being used. It is now proposed that both the feeder will be used for the entire facility on a hot standby mode.
- ii. A metering panel is available but has been defunct since long and not been in operation. The Bidder needs to offer two new metering panels with all accessories.
- iii. The HT cable from the Pole to the metering panel, from metering panel to the HT panel and from HT panel to the Transformer need to be replaced if required by considering the ratings.
- iv. The transformers need to be replaced with higher rating of 3 MVA. It will be a dry AN type transformer.
- v. Bidder must propose for replacement of Bus Bar trunks (BBT) from Transformer to the transformer output panel with a higher rating.
- vi. The entire job is turnkey type. However, the bidder has to submit a detail bill of material with prices for each item and quantity.
- vii. All the work must be done as per central and state electrical guidelines and under strict supervision of OCAC and electricity board authorities.

- viii. The bidder may engage an Electrical contractor to get the job done. The contractor must have a Class-A electrical license and must have qualification and experience of working on 33KV HT setup as per the state government statutory requirements.
- ix. Adequate safety procedures must be adopted while doing the execution work for HT and HT side as per the prevalent and suitable norms and law of the land.
- x. Bidder must offer a buyback price for the replaceable items such as Metering panel, HT panel, Transformer, BBT, HT cable etc. This will be taken in consideration during commercial evaluation.
- xi. During the replacement and installation activity, bidder must ensure that backup power is provided to the facilities of OCAC and OCAC tower. No interruption will be permitted during working hours. However, in unavoidable circumstances, in case any shutdown of services is required, the same may be intimated to OCAC, discussed and agreed upon before execution of the plan. For the same, bidder may propose/consider for deployment of mobile DG set of the desired capacity during execution/migration activity at their own cost including fuel consumption.
- xii. All CEIG & other mandatory statutory/Government approvals to be taken care by the bidder. However, OCAC will pay the statutory charges.

#### 5.6. Diesel Generators

- i. For captive power back-up system, Diesel power generators must be proposed with all its ancillary supplies such as Buffer storage and Bulk storage tanks, Exhaust system, Fuel piping system etc. The diesel generator must be Data Centre continuous type. The DG must be capable of taking the loads of existing Data Centre in OCAC building and proposed Data Centre in OCAC tower.
- ii. It is proposed that 1.8 MVA Data Centre continuous rated diesel Generator set is required. However the bidder must consider the exiting load and proposed load to arrive at the rating and the same may be verified and approved by Uptime.
- iii. The generators will be in N+N configuration where N is the total load.
- iv. The generator may be installed at the existing place where already 3 generator sets are running for SDC-1. In case the space is not sufficient for 2 nos of new sets, at least one of the set be placed in the same place and the other one in a different place as mutually agreed between the bidder and OCAC. Double tier stacking of DG may also be explored as an option.
- v. Existing exhaust systems needs to be dismantled and a new exhaust system be erected as per CPCB norms. In case self-supporting structure is required for the exhaust, the same must be proposed.
- vi. Adequate fuel pump mechanism is required for pumping fuel from the tank to the generators. The pumps and piping must be redundant & as per desired standards.

- vii. Intrinsically safe fuel meter must be installed on the fuel pipeline with provision of sending real time consumption data to monitoring tool such as DCIM.
- viii. A shed must be created over the DG canopy to protect it from rain & heat. The shed must be made with GI angles and PVC sheets or by any other material which is strong ,durable and can sustain local historical wind velocity due to cyclonic storms.
- ix. The underground HSD tank must have adequate safety provision as per CCOE.
- x. Cables from the Generators may be laid inside the existing trench. In case trench is not available, a new trench may be created as per the existing norms.
- xi. Existing DG set foundation must be dismantled & fresh DG foundation need to be created as per OEM specification if it is decided that one of DG is placed in existing DG location

### 5.7. MV Panels

- i. The entire building has to have a comprehensive power distribution design where LT panel will be an integral part. The same will be used to feed power to the critical and non-critical areas. These panels may include Main LT panels, Distribution panels, Power factor panels etc. For the server farm area, there will be two LT panels placed at different rooms to provide physical redundancy. The panels will be fully compartmentalized (form 4b) and modular.
- ii. The transformer output panels must be replaced with higher rated breakers and protection. The old panels has to be taken back by the bidder with a buyback offer.
- iii. Existing APFC panel need to be upgraded to suitable capacity of Capacitor banks. Bidder need to design the capacitor bank & evaluate the existing panel for installation of desired rating of capacitor banks. If required bidder can propose new APFC panels with buy back offer for existing APFC panel.
- iv. The bus bar from the transformer output panel to the ASLS panel will remain as it is. The bidder must properly study the location and placement of these Bus bar so that connection between the new output panel and the bus bar does not throw a challenge. In case the Existing Bus bar does not fit into the design of the bidder, then the bidder can propose new bus bar with different rating with justification. In this case the existing bus bar must be taken back by bidder with a buy back offer.
- v. In similar manner the cable that is feeding the SDC-1 from the transformer output panel should not be replaced once a new panel is installed. The same cable should be connected to the new panel. This essentially mean the new transformer output panel must be designed in a such a manner that the output cable ally of the panel is suitable to accept the existing cable termination.
- vi. The existing cable from the DG yard to the DG sync panel will be removed by the bidder.

- vii. The DG sync panel already in working will have to be removed by the bidder and a buy back offer must be submitted. This panel will not be required in new scheme.
- viii. There will be 2 new DC LT panels to be proposed by the bidder as the block diagram shown.
- ix. All interconnecting cables must be proposed. All panels must be type 4b form factor panels.
- x. There will be HVAC panels inside the Data Centre power room from where the PACs will be powered.
- xi. There will be UPS output panel with Isolation transformer placed inside the Server hall. This will be redundant in nature. The input and output connection will be through cable.
- xii. The bidder should propose additional auxiliary panels/DBs as per the data center standard such as Emergency Panel, Lighting Panel, Comfort AC panel, Raw power Panels etc. for better distribution of power in a mission critical facility.
- xiii. The DG output panel as per the scheme is proposed to be placed near the DG. Since it will be outdoor, the panel must have ingress protection level IP 68. This will be placed on a PCC foundation.

#### 5.8. UPS Systems

- i. For uninterrupted power supply UPS with battery bank of required rating must be proposed for the Critical and Non-Critical load. The UPS must be modular and can be scaled up vertically and horizontally including static bypass switch. The battery backup system should be for 15 minutes. Battery has to be lithium Ion type. A separate UPS bank system has to be provisioned for support area.
- ii. The UPS system will be placed in two different power rooms with its individual battery banks.
- iii. The UPS system has to be connected to the DCIM for real time performance monitoring.
- iv. UPS system has to be modular in such a manner that the modules can be replaced safely without any arching.
- v. Bidder must submit battery calculation sheet.
- vi. The bidder must propose UPS systems with minimum footprint.
- vii. The UPS must be with maximum efficiency and minimum THDi. The output power factor must be closest to unity.

#### 5.9. Cable, Bus Bar Trunks and Terminations

- i. Cables and Bus bars of different types and sizes as per the required design for connecting all required components from source to load or vice-e-versa with termination at both ends. Indoor bus bars to be installed inside the server farm for Rack power.
- ii. All outdoor cables will be Aluminum core and all indoor cable will be copper core.
- iii. The bidder must submit cable schedule as per the following format.

### 5.10. Cable Schedule

The bidder has to submit a detailed schedule of cables and bus bars in the following format.

Sl. No	From	To	Max Amp	Cable Ampacity	Cable Size in sq mm	No of cores	Type of core	No of runs	Insulation	Length	Qty
01	A	B	500	700	185	3.5	AL	2	XLPE	50	100

- Description of headers:

From – The point from where cable/BBT is starting

To – The point from where the cable/BBT is ending

Max Amp – The maximum load current per phase that the cable/BBT has to carry

Cable Ampacity – The maximum current per phase the cable/BBT can handle

Cable Size: Size of the cable in sq mm

No of Cores: Number of cores of cable per segment (e.g. 1, 2, 3, 3.5, 4 etc.)

Type of Core: The metal type used (e.g. Aluminum, Copper)

No of Runs: Number of cable segment that has to run between two segments

Insulation: Insulation of the cable (e.g. PVC, XLPE etc.)

Length: The distance between starting and end point of the segment.

Qty: Total cable quantity (Length x no of Runs)

### 5.11. Cable/Conduit/Bus bar Laying

- i. The bidders are strongly advised to maintain data consistency between Electrical Single line diagram, Cable schedule and Bill of quantity at all times in the solution document. The Electrical Single line diagram must be prepared in detail showing all the components. All the components must be uniquely labelled.
- ii. All cabling inside the server hall will be over the top of the racks.
- iii. Track busway continuous BBT has to be used for IT racks. From UPS Output panel till end feed unit of bus bar cable will be used on cable tray.
- iv. All conduits inside the server hall will be MS type. No PVC conduit will be accepted. However, the conduits if laid inside the wall can be PVC with FRLS type.
- v. There has to be raw power provisions inside the server hall at every 10 mtr for facility maintenance.
- vi. All cables must be tagged with unique name. The tag must be long lasting and durable. Tagging has to be on both ends.
- vii. All cable entry to the panels must be with double compression glands. The glands must be chosen as per the cable core metal.
- viii. Cable installation must be as per IE rules considering pull strength, bending radius and insulation class.
- ix. All outdoor cables must be factory tested in presence of OCAC authorities for insulation strength.
- x. All outdoor cables must be XLPE and all indoor cables must be FRLS Type.

- xi. All wiring in the support area must be concealed. Sub-mains must be laid in PVC raceways buried under the PCC floor. The distribution to the desks must be through the furniture raceways from bottom.
- xii. There must be junction boxes on the floor under the carpets or on vitrified tile floors. It must be concealed but should be openable for maintenance.
- xiii. UPS output cabling must have double neutral. Single core Cu cable must be used.
- xiv. Cable end point insulation has to be by heat shrink sleeved. Taping will not be allowed.

### 5.12. Illumination

- i. Lights of various types as suitable for different floors including critical and Non-Critical areas are required to be done. Lux level inside server farm to be 500 lux measured at 1 mtr from ground at all area. Other area should have 300 lux. Lux Level Map from manufacturer must be submitted before execution.
- ii. Bidder must propose LED lights of different sizes as suitable and approved by OCAC.
- iii. All the lights will have occupancy sensors.
- iv. Bidder may propose different size of light as per the suitability and ambience required.
- v. The light fixtures in the support area will be recess mounted on the ceiling. The lights on the server hall and power room may be suspended from ceiling without compromising the aesthetics.
- vi. The size for fixtures can be chosen by the bidder so that the looks and ambience is not compromised

### Wall Outlets, Outlets for Racks, Receptacles:

- i. End point power outlets are required for all load points depending upon type and redundancy.
- ii. The wall distribution panels must be double door type and recessed on the wall.
- iii. The looping of raw power and UPS power points for the user is allowed. However not more than 3 raw power points and more than 2 UPS power points be looped for a single circuit.
- iv. The receptacles on the wall and on the desk must be high durable and multi-pin type. Each desk must have 3 sockets, one for raw power and two for UPS power with proper levelling.
- v. The breakout and canteen area must have 5/15A power sockets 5 nos.

### 5.13. Grounding/ Earthing

- i. Earth pits of different types, grounding bus bars/strips, Equi-potential grid for the critical area.

- ii. There are many earth pits already existing in the campus. For new DG area, the earth pit may not be required and the existing earth pits may be used. However in case of fresh requirement the same may be provided. All earth pits irrespective of Copper or GI have to be chemical type.
- iii. Earth pits may be required for UPS systems and other items inside the Data Centre. The same may be proposed by the bidder.
- iv. The server hall must have grounding mesh in terms of Copper strip or braided copper wire laid on the ground or above the ground on a matrix fashion to provide equipotential grid for all the equipment.
- v. Each and every metal item inside the Data Centre must be grounded.
- vi. The earth strips have to be copper for copper pits and GI for GI pits. All the earth strips must be insulated.
- vii. All the critical equipment (like UPS, DG set, Transformer etc.) earthing must be of copper plate type with copper strips of required specification.
- viii. All the earth pits must be covered with required standard of earth pit covers with recommended load bearing specifications of OEM.
- ix. Interconnection of earth strips has to be by welding in alloy material or by non-corrosive nuts and bolts.
- x. Earth pits must be connected at ground for redundancy and equi-potential.
- xi. The complete earth works like excavation, refilling & RCC covers of the desired standard will be in bidder's scope.

#### 5.14. Cable Pathways

- i. Various pathways such as underground trench, cable trays, Raceways, junction boxes, ladder trays, and Cable baskets required to be there for the entire facility.
- ii. The existing trenches must be used for outdoor cable pathways. In case of the existing trenches are not sufficient, bidder can propose new trenches.
- iii. In case of new trenches, the complete earth works like excavation, refilling & RCC covers of the desired standard will be in bidder's scope
- iv. Cables must be taken to Data Centre from ground area by designated shaft. All cables must be tagged.
- v. Inside the Data Centre all cables must run over the rack on cable tray.
- vi. Inside the power room call cables must run cable trays over the top.
- vii. Cable tray must be factory made with pre-galvanized finish.
- viii. Cable fill in any tray must not be more than 60%.
- ix. All cabling and wiring must be neatly dressed and tagged with unique identity.

- x. Existing shaft for power cable must be used for taking cables from outside to inside the floor. While working on the shafts, adequate care must be taken not to disturb other cables running inside it.

**a. Wiring**

- i. Wiring of all load points, wall outlets, Lights and all other points where connection is required.
- ii. All along the Data Centre area, wiring color codes must be used for single phase, three phase and Ground. All wires and cables must tagged with unique identity.
- iii. No jointing of cable or wires are allowed without proper factory made jointing kit.

**b. Cable Entry**

Fire resistant (factory fabricated) cable/pipe entry blocks at walls must be used. The same type of entry block must be used for the pipes as well.

The reference image is shown below:



Fig. No-16

**Documentation Submittals:**

The bidder must submit the following in various stages of the project:

- i. Complete unpriced BOQ according to the bidder's solution- To be submitted along with technical bid.
- ii. Single line diagram – To be submitted along with bid. The single line diagram has to be in detail showing unique notations for each and every component such as breakers, indicators, CTs, bus bars, cable rating etc.
- iii. Cable schedule as per the format. – To be submitted along with bid.
- iv. Lux level calculation – To be submitted along with bid.
- v. Cable and panel datasheets – To be submitted long with bid
- vi. Shop drawings for cable pathways, wiring, and RCP – Before execution
- vii. Coordinated drawing – Before start of execution



### 5.15. Scope of work – HVAC system

- PRECISION AND COMFORT AIR CONDITIONING

- i. Technical area such as Server farm, Power rooms will have precision cooling system.
- ii. The server farm is proposed to have 10 row of racks with each row of 9 racks where each rack size is considered to be 800mm x 1200 mm.
- iii. There will be cold aisle containment for racks and hence there will be 5 containment PODs. Each POD will consist of 2 row of racks.
- iv. One of the POD of 18 racks will be high density racks. There will be direct expansion in-row cooling for this POD. It is suggested to have 8 in-row cooling units, with four in each row. The eight units are in N+1 redundant fashion where N=7. However design ownership lies with bidder.
- v. All other row of racks will also have in-row cooling as well. It is suggested to have 6 units in N+1 redundant mode where N=5 per row. Bidder must proposed the rating of the units in such a manner that not more than 6 units are required for a POD for 18 racks and foot print of the units combined is limited to 1800mmx1200mm.
- vi. The cold aisle containment should be proposed in such a manner that a maintenance corridor is created in between the PACs and the rack row. This can be possible by proposing sliding doors on the one side (PAC side) hot aisle of the row.
- vii. All the refrigerant piping must run on the side of the wall below the raise floor and go out of the facility at the middle point through the balcony to the ODU platform.
- viii. Pipes have to be properly insulated. The exit of the pipes on the wall must be through factory made sealing blocks with fire rated material.
- ix. The outdoor stand to be made behind the building on ISMB/ISMCs with access from ground through a staircase. The height of the platform to be 5 mtr. from the ground level so that fire tender can pass through it.
- x. Adequate safety barriers must be taken care of on the platform on all sides. Portable fire extinguisher must be installed on the platform.
- xiv. Humidifier line can be taken from building water pipe line with a valve.
- xv. For the DC support area, the entire area to be provisioned with VRV/VRF system where the outdoor units will be placed on the ODU platform.
- xvi. The indoor units on the DC support area will be cassette type. Bidder must submit a heat load calculation along with detail BOQ in the technical bid.

- xvii. Bidder must submit a detail table of selection of various rating of indoor units with its cooling capacity in terms of CFM, power consumption and size.
- xviii. Power room will have PAC units (floor standing) without heater and humidifier. Bidder must consider the equipment heat load, room area load and latent heat for selection of rating of the units.
- xix. Power room PAC will be redundant as per Uptime guide lines.
- xx. Bidder has to submit a detail bill of material with prices for each and every item.
- xxi. All the AC (PAC & VRF) units must have provisions to connect to DCIM. It must also be connected to the fire alarm system for tripping during fire.
- xxii. One of the AHU has to be removed out to of the floor completely and the chill water pipes be closed with end cap. The same room will be converted into a power room.
- xxiii. Bidder must propose thermal insulation (under deck insulation) on the server hall floor and ceiling and on the support area. The thickness of the insulation must be min 23 mm and material to be nitrile rubber.
- xxiv. It may be possibility that the pipes from the indoor units of the DC support area has to run through the server hall under the raise floor. This may be avoided. In case it is a must then, the same may be done with proper workmanship.
- xxvi. Power to each PAC indoor units will be from two different HVAC panel. The bidder may propose an ATS with two inputs and one output for each PAC incase the PAC do not have provisions for 2 inputs.

## 5.16. Scope of Work – Safety, Security, Surveillance and Monitoring System

### 5.16.1 Addressable Fire Alarm System (AFAS)

- i. Entire facility will have fire detection, annunciation & Alarm system. Different types of detectors such as fire, smoke and heat detectors or combination of all installed and wired to a control panel in a zonal fashion.
- ii. This system must be integrated with the central monitoring system. The fire panel must have redundant components inbuilt.
- iii. The first floor of the proposed site already have fire hydrant system and pipes are running all across the floor. The bidder has to disconnect and dismantle the pipes in server farm area only. This area will be replace by Novec agent in place of water as a fire suppressant.
- iv. The fire hydrant on the support area side will remain as it is and it will remain connected to the main system.

- v. The nozzles of hydrant system in the support area will be extended till the false ceiling level.
- vi. The AFAS system will have manual call points, hooters and all other accessories for complete fire detection system.
- vii. There must be a provision to connect the system to the building main fire alarm system
- viii. Illuminated exit signs must be installed on all possible points.
- ix. Emergency evacuation laminated chart of A3 size must be displayed at all important locations.
- x. A fireman's boot, safety jacket, goggles, gloves, hammer, Axe etc. must be kept in a steel fabricated case with front face visible.
- xi. Detectors must be placed on all voids.
- xii. A detail table of items must be submitted with quantity and type of items.
- xiii. The design will be as per NFPA and local fire codes whichever is applicable.
- xiv. Hooter with strobes are to be installed at least 4 points in the Data Centre area.
- xv. The bidder should submit detail design sheet as per the OEM recommendations along with the bid.

#### 5.16.2 Aspiration Smoke Detection System or Very Early Smoke Detection System

- i. VESDA system may be required in the server farm area & power rooms for early detection of smoke with a facility of alarm.
- ii. The system must be digital and the panel has to be installed inside the BMS room
- iii. The sampling pipe has to run over the PACs and below the floor if required.
- iv. The detectors has to be placed inside the containment as well.
- v. The bidder should submit detail design sheet as per the OEM recommendations along with the bid.

#### 5.16.3 Gas Based Fire Suppression System

- i. The technical area such as Server farm area, UPS room, Panel and battery room must have fire suppression system with an alarm such that in case of fire the gas agent gets released through the nozzles and suppress the fire fully without damaging the electronic devices.
- ii. There will be three separate suppression systems. One for server hall and one each for 2 power rooms.
- iii. The suppression nozzles must be placed on all voids and including the inside of containment.

- iv. The cylinder has to be seamless type.
- v. In case there is a flooding of gas during execution and before the site handover bidder need to replace the gas at its own cost.
- vi. Placement of cylinder bank is shown on the layout.
- vii. The gas based suppression system must be integrated to fire alarm system
- viii. Pressure on the cylinder must be maintained throughout the contract period.
- ix. There should be provision for integration & monitoring of cylinder level pressure in the DCIM.
- x. The bidder should submit detail design sheet as per the OEM recommendations along with the bid.

#### 5.16.4 Close Circuit Television System (CCTV)

- i. Surveillance of inside and outside of the facility must be done with different type of IP cameras such as fixed/Dome/PTZ high definition cameras with facility of motion based recording for one month in inbuilt HDD and video analytics.
- ii. The cameras inside the server hall to be for all the aisles including the containments.
- iii. No area must be left out of surveillance except the washrooms, manager cabins, and bunk bed room.
- iv. The staircase, ODU platform, DG area, HSD tank area, Utility area have to be covered under CCTV system
- v. All cameras have to powered by CAT6A from POE switch.
- vi. At least three PTZ cameras must be proposed for outdoor in addition to fixed cameras.
- vii. Recoding must be archived for 6 months in an external drive supplied by the bidder.
- viii. At least a month recording must available in NVR in inbuilt HDD.
- ix. All recording have to motion based inside the server hall. However inside the Power rooms it has to be continuous.
- x. The boundary wall behind the building on the Data Centre portion also need to be covered under CCTV.
- xi. The bidder should submit detail design sheet as per the OEM recommendations along with the bid.

- xii. The bidder should evaluate the existing CCTV system of OSDC 1.0 & propose the solution in such a manner that the existing CCTV system can be integrated with the proposed CCTV system of OSDC 2.0.

#### 5.16.5 Access Control System

- i. Access to the facility has to be controlled. Dual Electronic authentication on each entry to the critical area must be there. Physical access controlled (manned) also have to be configured wherever required. The scope will include all the access control system mechanisms including authentication, prioritization and monitoring. Turnstiles, flap barriers, swipe barriers are part of access control system scope.
- ii. All the doors have to be controlled by access control hardware and software.
- iii. All doors must have entry and exit card reader.
- iv. Server hall entry must be with biometric access from people entry side and card reader entry from material entry side.
- v. There has to be a full height turnstile on the entry of server hall with an adjacent fire rated glass door.
- vi. There has to access flap barriers (2 nos ) at the entry of the facility near the passenger Lift area
- vii. A full height metal detector must be installed near the entry.
- viii. An x-ray baggage scanner must be installed at the entry of the facility.
- ix. A comprehensive visitor management system must be installed with computers, cameras and card printer near the security area at the entry of the facility.
- x. Access control software and required computer has to be a part of the scope of the bidder.
- xi. A detail design sheet as per OEM recommendations must be submitted along with the bid

#### 5.16.6 Water Leak Detection System

- i. Detection of water and other liquids at the pipes those are used for flow of the same or at the floors where ever there is possibility of water or liquid leakage with detection and alarm system
- ii. Water leak detection cable must be run near all water pipe lines inside the server hall and power room.
- iii. Water leak detection system must be digital type with a hooter connected to the system.

- iv. The complete system shall include an electronic System control panel, multiple control modules , distance type sensing cable and all required auxiliary accessories (such as hold down clip & Tag/Label for the sensing cable).
- v. This system shall detect and locate multiple leaks simultaneously as well as cable break & power failure and activate the control panel alarm relays. The sensing cables shall be of such construction that no metallic parts shall be exposed to the environment. The system shall be provided with the flexibility of custom "cut-to-length" sensing cable to meet the exact length requirement at each area of protection and with pre-connectors sensing cable components.
- vi. Water leak detection system must have capabilities to integrate with monitoring tools like DCIM.
- vii. A detail design sheet as per OEM recommendations must be submitted along with the bid

#### 5.16.7 Rodent Repellent System (RRS)

- i. Ultrasonic frequency based electronic system to repel rodents from the floors with help electronic wave emitters.
- ii. The satellites of the RRS to be installed in all voids in server hall, support area and power room.
- iii. The RRS must capable of integration with DCIM tool for monitoring the health of satellites & Transducers.
- iv. A detail design sheet as per OEM recommendations must be submitted along with the bid.

#### 5.16.8 Data Centre Infrastructure Management Tool

A comprehensive tool to monitor all the services and products installed in the facility. All the field devices have to be monitored though DCIM. The bidder should evaluate the existing BMS system of OSDC 1.0 & propose the solution in such a manner that the existing BMS system can be integrated with the proposed DCIM system.

#### 5.16.9 Visitor Management System

A comprehensive visitor management system need to be in place for the proposed Data Centre. This has to be image based access. The software must be integrated with the Door access control system for unified authentication. Every visitor will be issued a photo I card with a lanyard. Computer, i-card printer, camera and software is part of the bidder scope.

**General Note:** The bidder is not required to submit the drawings for any of the above systems with the bid. However following documents are mandatory

1. Design Sheet as per OEM recommendations.
2. Bill of material with quantity and price.
3. Datasheets.
4. Compliance to SOW and Requirement.

#### 5.17. Scope of Work -Network Passive Infrastructure, Racks, IPDU, etc.

- Fiber and copper cabling as per TIA/EIA guidelines
- Tier III compliant and Tier 4 ready design
- 25 years certification.
- Fiber cabling will be through fiber runner and copper cabling in the cable basket, all over the racks.
- All racks to be supplied are 800mm x 1200mm with access control system in-built. All are perforated racks and of 42U size.
- Each rack will have two numbers iPDUs those will be connected to DCIM for port level monitoring.
- A asset tracking software tool must be installed to track the real time assets
- The iPDUs will be connected to the tap of box of track busway system
- Each row has to be provisioned with a network cum passive rack at end of the row
- Copper cable has to run on cable basket and fiber on fiber pathways/fiber runner.



Fig. No-17

- Each desk in the support area will have two data ports and one voice port.
- Entire voice cabling will be on Cat6A.
- At least 15 nos IP phones must be supplied for the entire facility.
- An IP EPABX has to be supplied and installed in the facility.
- Cat6A cabling on the support area has to run under the floor on PVC raceway.
- Bunching and bending radius of the cable will be as per manufacturer standard.
- The racks those are not used or U space that is not used, will have blanking panels on them.

### 5.18. Upgradation of Utility equipment, integration and commissioning

The facility has 33KV substation with VCB panels, transformer and many other panels. Many of the equipment are proposed to be upgraded/ replaced and are under scope of the bidder. In the execution phase the installation planning and execution has to be done in such a manner that no disturbance happens on existing load. The bidder may use the existing DG sets of OCAC tower (4 nos) and SDC (3 nos) to feed the load during execution. There may be a scenario where a mobile DG has to be stationed at the facility during integration process. The same may be arranged by the bidder at their own cost. Also it may happen that temporary cables, accessories and breakers/panels are required for the integration. The same may be arranged by the bidder at their own cost.

The bidders are advised to do a thorough study of the facility before bidding. The integration methodology will be part of scope of the technical presentation and will be an evaluation criteria. The bidder is advised to create presentation slides with step by step approach of the integration with timelines.

### 5.19. Tier Certification by Uptime Institute

The bidder has to ensure that the Data centre gets certified for Tier III or higher as feasible and suitable from Uptime Institute Inc.

The Data Centre Facility to be constructed under this contract shall be Uptime Institute Tier III/Tier IV Gold Certified. The successful bidder shall obtain the following as part of this certification process:

- Tier III/IV Certification of Design Documents for Complete Data Centre Facility Design
- Tier III/IV Certification of Constructed Facility for all areas of Data Centre Facility to be constructed under this contract
- Tier III/IV Certification of Operational Sustainability.
- All Certifications shall be kept valid for the contract period
- The necessary certifications will be obtained on the behalf of the client and passed on to them on award.
- Bidder has to offer rates for all three certifications separately.

### 5.20. Data Centre Health Check Audit

#### **Need of the Audit:**

In a dynamic scenario that the Datacentre always is, technology changes keeps on happening on a continuous manner. Form factor of the IT equipment keeps on changing to the lower side to get itself accommodated in more numbers in a rack. However at the same time more computing and processing capacity inside the equipment amount to drawing of more power from the source. It may not a difficult task to design the facility that can feed more power to the equipment. However cooling the equipment due to high and dynamic heat rejection is always a challenge.

Once a Datacentre is made and commissioned, IT equipment (hardware) gets added every now and then. It is important to be aware about the health of the facility in terms of power and cooling due to the continuous changes in Rack population status in the Datacentre and overall power and Thermal status.



### **Audit Methodologies:**

The auditing firm must follow the procedures as follows for the Audit. Instruments to be used for the data collection may be as follows

- Prepare an Audit project plan and submit to the client for approval
- The plan must indicate the system down time if required. However, no system down time should be required while doing the audit.
- Data collection points through instruments must be mutually agreed with client
- Class A power Analyser must be use to capture performance data.
- Power Audit Method
  - Transformer Visual checks for Oil and temp level, grounding, Vibration checks
  - Data logger on transformer output side for 24 hours
  - Data logging for all major output breakers of Main panels
  - Earth Resistance checks
  - Harmonic analysis till 11th harmonics
  - UPS input and output data collection for V,I,HZ,KW,KVA,KVAR, unbalance, harmonics
  - Ampacity of the cables, BBT used.
  - Diesel generator SEGR calculation
  - Vibration and Noise level checks for generator
  - Diesel generator output data logging.
  - Thermal imaging for all major breakers from Source to load.
  - Thermal imaging analysis.
- HVAC audit method
  - Temperature inlet and outlet of each precision air-conditioner (PAC)
  - Temperature data logging for each PAC for 4 hours
  - CFM measurement at each opening.
  - Power data logging for each PAC for 30 minutes.
  - Chiller and pump data collection visually.
  - Chill water flow data through ultrasonic method.
  - Complete analysis of the thermal stability.
- IBMS system audit method
  - Complete visual checks for all field devices
  - Simulation through induced method
  - BMS/DCIM details checks and analysis

Following measuring instruments must be used for the above tasks

- Class A power quality Analyser
- Air hood or Balometer
- Thermal Imager
- Temperature loggers
- Vibration meter
- Noise level meter
- Lux meter
- Earth Resistance meter
- Clamp meter and Multimeter.

### **Audit reports and Documents:**

Post the data collections the Auditing firm must do a detail analysis on the data collected from the field devices and create a report that must depict the following

- Visual inspection report
- Report generated by the Analyser
- Thermography report
- Complete analysis report based on the measuring instrument data
- Risks and mitigation suggestions
- Safety reports
- Energy efficiency report.

The successful bidder shall be responsible for all associated cost for obtaining & maintaining these certifications.

#### 5.21. Indicative List of Equipment need to be considered for Buy Back option

S.N	Equipment	Rating	Quantity	Make /Model If any	Additional Info	Remarks
1	HT Metering Panel with CT PT	33 KV	1	NA		
2	Main HT Panel	1 X 36 KV, 800 A VCB 2 X 36 KV, 800 A VCB	1	Jyoti		
3	Transformer	1600 KVA	2	OEU	HV Voltage: 33 KV, LV Voltage: 433 V, HV Current: 28 Amps, LV Current: 2133.4 Amps	Indoor Type, ANAN with on Load Tap changer
4	Transformer Splitter Panel	I/C : 1X2500 Amps ACB, O/G: 2X2000 Amps ACB	2		2500 Amps Aluminium BBT is connected from transformers to splitter panels.	
5	400 KVA Diesel Generator	400 KVA	3	Kirloskar KG400 WS	SI Nos: KV85001/1000170 KV85001/1000195 KV85001/1000165	
6	External Fuel storage Tank.	1000 Litres Capacity	3			
7	DG AMF sync cum auto Management panel	I/C: 3X630 Amps MCCB O/g: 2X1000 Amps ACB Bus coupler: 2X 1000 A ACB	1		PLC Make: Woodward	

N.B: The above list is only indicative & not exhaustive, the bidder should visit site to evaluate the actual condition & detail specification of the equipment's earmarked before quoting the buyback price.

## 5.22. Technical, Functional and Operational requirements of Equipment's (Non IT):

### 5.22.1 Uninterrupted Power supply (UPS) system with Battery back-up (For Critical Load)

**Rating/Sizing: 2 x 400KVA – 2 sets**

#### Product/Solution Description

There will be 2 set of UPS systems, each to be connected in one path of power to the Data Centre. The UPS are to be modular in nature with vertical and horizontal expandability. The frame size shall be minimum 150 kVA/200KVA or above and Module size shall be 20 kW to 50 kW. Each UPS should have N+1 modules. Failure of one module in each Frame shall not take down entire Frame but only for the failed module capacity. This is applicable for UPS Frames of operating in parallel configuration i.e. only the failed module capacity shall be isolated with remaining modules in parallel frames operating normally. The 3 Phase UPS modules comprising of rectifier, Inverter, charger etc. must be swappable. It shall be possible to plug out the Healthy or Faulty UPS sub module from the frame in normal Online Double Conversion operation.

Battery bank to be Lithium Ion standby application type. Each UPS must have battery backup for 15 minutes considering load power factor of 0.9 till end of 5<sup>th</sup> year. Lithium Ion chemistry to be used shall be LMO-NCM only.

#### Scope of Work

1. Supply of UPS systems Unloading, shifting, Storing, Installation, Testing and Commissioning.
2. Supply of Battery banks Unloading, shifting, Storing, Installation, Testing and Commissioning.
3. Providing training to Client and maintenance team.
4. Periodic maintenance.
5. SLA adherence.
6. Repair and Replacement if required.
7. System Acceptance test at Factory and at Site.( on full load condition)

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	Efficiency on Online mode to be $\geq 98.5\%$ along with PF Correction to Unity at Input & Harmonic Correction (THDI) to $< 3\%$ at Input and simultaneously Battery Charging also. From load range of 50 to 100%.		
2	Input Power Factor must be 0.99 at load $>25\%$		
3	Total current harmonic distortion to be 3% or less at 100% rated load		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
4	Battery to be Lithium Ion and back up must be 15 minutes on full load per UPS at 0.9 load power factor till end of 5 <sup>th</sup> year. Battery sizing calculation must be submitted duly endorsed by battery manufacturer. Lithium Ion battery with LMO-NCM chemistry shall be provided		
5	Battery System to be equipped with cell, module, bank level battery management system and to be monitored by Data Centre Infrastructure Management system with following certifications: Safety Cell UL1642 , Module UL 1973 , Seismic GR63 EMC IEC61000-6-2 , 61000-6-4		
6	UPS must handle 100% unbalanced load		
7	<ul style="list-style-type: none"> <li>▪ Nominal Voltage</li> </ul> Input: 380/ 400/ 415 VAC - Three Phase four wires + ground  Output: 220/380, 230/ 400, 240/415 VAC (Selectable) - Three Phase four wires + ground		
8	Each pluggable type, swappable and user replaceable Power module should have its own full rated rectifier, full rated inverter, static bypass switch & battery charging circuit.		
9	Each UPS should be comprising of Inbuilt Input, Output, Static and Maintenance Bypass switches rated for 100% capacity. UPS should have redundant power supplies, redundant controller, in case of failure of one controller there should not be any impact on UPS capacity.		
10	Input Voltage Range: +/- 15% (On Full Load)		
11	No derating in UPS capacity from 0.6 leading to 0.6 lagging of load power factor.		
12	Rectifier to be IGBT based and Inverter to be IGBT based ( 3 level or better) (Switching losses Shall be Less than 30% on IGBTs)		
13	The Modules should have Redundant variable speed fans and capable of maintaining the system in event of single fan failure.		
14	The Modules should be mounted on to safe back plane of separate AC and DC power without use of any interconnecting power cables.		
<b>Desired Technical Requirements</b>			

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
1	Noise level should be less than 65 db on normal condition at 1 mtr distance		
2	Smaller foot print (Individual UPS Frame depth & width shall not exceed from 850 mm & 550 mm)		
4	The UPS should have built in facility through which it can be switched off immediately through local switch or remote Emergency Power Off switch wherein the load is disconnected from the UPS under emergency condition. Restarts are possible after manual inspection and removing the conditions of emergency and resetting the Emergency Power Off switch.		
5	UPS should have a wide choice of communication interface through SNMP / Modbus protocol using the RS232 / RS485 / Ethernet port.		
6	No deration in UPS capacity ( KVA and KW) from 0 to 40 deg C operating temperature		
7	The UPS should be <b>UL/CE</b> Listed.		
8	Phase Correction/Corrector required (Inbuilt or External)		
9	Back feed protection required (Inbuilt or External) at Mains as well as Bypass		
10	Energy Meter for displaying kWh consumption (Inbuilt / External)		
<b>OEM Qualification Criteria</b>			
1	Manufacturer Authorization letter (As per format) to be submitted along with technical bid. ( Note: Only one OEM allowed)		
2	Must have operational service centre (Since last 5 years) in Bhubaneswar or within 50KM radius of site. Bidder to provide proof of address of facility in form of GST registration/MOA/Company or farm registration		
3	At least 50 installation in India for the offered rating. Proof in form of purchase order either in name of Bidder or OEM to be furnished. Install Base of Minimum 50 Racks of Lithium Ion with 100 kW and above UPS ratings		
4	The OEM must have been in production, supply, and maintenance of UPS systems at least for 10 years till the submission date of the tender. Proof of facility in form of GST		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	registration/MOA/Company or firm registration or self-declaration signed by head of Production unit.		
5	The OEM must have manufacturing facility in India for the UPS rating provided. Proof of facility in form of GST registration/MOA/Company or firm registration or self-declaration signed by head of Production unit.  Note: Declaration for Sl.3 and 4 can be a single letter.		

**Evaluation Criteria (Critical UPS):**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Critical UPS	2	AC Efficiency	>96%	0.5
				95% to 96%	0.15
			IGBT Inverter Level	> 3	0.4
				2 to 3	0.15
			Power Module Rating	>25 KW	0.4
				<25 KW	0.15
			UPS System	UL/CE Listed	0.4
				Non UL/CE Listed	0.15
			LIB System(Cell and Module and System)	UL Listed	0.3
				Non UL Listed	0.25

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

### 5.22.2 Uninterrupted Power supply (UPS) system with Battery back-up (For Non-Critical Load)

**Rating / Sizing: 2 x 20 KVA – 1 set**

#### Product/Solution Description

There will be 2 set of UPS systems, each will be connected in one path of power to the Data Centre non critical load. The UPS are to be unitary/monolithic in nature with double conversion IGBT based technology.

Battery bank to be VRLA/SMF standby application type. Each UPS must have battery backup for 30 minutes.

#### Scope of Work

1. Supply of UPS systems Unloading, shifting, Storing, Installation, Testing and Commissioning
2. Supply of Battery banks Unloading, shifting, Storing, Installation, Testing and Commissioning
3. Providing training to Client and maintenance team
4. Periodic maintenance
5. SLA adherence
6. Repair and Replacement if required
7. System Acceptance test at Factory and at Site ( on full load condition)

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	AC-AC Efficiency on normal mode to be 95% or better from load range of 30 to 100%.		
2	Input Power Factor must be 0.98		
3	Total Current harmonic distortion to be 5% or less		
4	Battery to be 12 V VRLA/SMF and back up must be 30 minutes on full load per UPS. Battery sizing calculation to be submitted duly endorsed by battery manufacturer.		
5	UPS must handle 100% unbalanced load		
6	<ul style="list-style-type: none"> <li>▪ Nominal Voltage</li> </ul> Input: 380/ 400/ 415 VAC - Three Phase four wires + ground Output: 220/380, 230/ 400, 240/415 VAC (Selectable) - Three Phase four wires + ground		
7	Each UPS should be comprising of Inbuilt Input, Output, Static and Maintenance Bypass switches rated for 100% capacity.		
8	Rectifier to be IGBT based and Inverter to be IGBT based.		
<b>Desired Technical Requirements</b>			
1	Noise level should be less than 65 db on normal condition.		
2	Smaller foot print		
3	Conformal coating of PCBA's		
4	Operating Temperature 0 to 40 deg		
6	UPS should have a wide choice of communication interface through SNMP / Modbus protocol using the RS232 / RS485 / Ethernet port.		
7	Dust Filter		
<b>OEM Qualification Criteria</b>			
1	Manufacturer Authorization letter (As per format) to be submitted along with		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	technical bid. ( Note: Only one OEM allowed)		
2	Must have operational service centre (Since last 5 years) in Bhubaneswar or within 50KM radius of site. Bidder to provide proof of address of facility in form of GST registration/MOA/Company or firm registration		
3	At least 10 installation in India for the offered rating. Proof in form of purchase order either in name of Bidder or OEM to be furnished.		
4	The OEM must have been in production, supply, and maintenance of UPS systems at least for 10 years till the submission date of the tender. Proof of facility in form of GST registration/MOA/Company or firm registration or self-declaration signed by head of Production unit.		
5	The OEM must have manufacturing facility in India. Proof of facility in form of GST registration/MOA/Company or firm registration or self-declaration signed by head of Production unit.  Note: Declaration for Sl.3 and 4 can be a single letter.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Non- Critical UPS	1	AC Efficiency	>95%	0.6
				94% to 96%	0.2
			UPS Unity Power factor 20 kVA = 20 KW	Available	0.4
				Non Available	0.2

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

**5.22.3 Precision Air Conditioning System (Direct Expansion In-ROW)****Rating / Sizing: As per Bidder's solution**

<b>Product/Solution Description</b>
-------------------------------------



The server farm area will be divided into 2 zones of 72 and 18 racks. There will be 10 rows and each row consisting of 9 racks. All rows will have in-row cooling with cold aisle containment.

**Scope of Work**

1. Supply of PAC (CRAC) systems Unloading, shifting, Storing, Installation, Testing and Commissioning
2. Supply of low side items required for PAC systems with Unloading, shifting, Storing, Installation, Testing and Commissioning
3. Creation of out-door unit platform ( Iron girder structure)
4. Providing training to Client and maintenance team
5. Periodic maintenance
6. SLA adherence
7. Repair and Replacement if required
8. System Acceptance test at Factory and at Site ( on full load condition)

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	Refrigerant – R410a		
2	<b>Compressor</b> : Step less capacity Modulation on time based engagement and dis engagement of the compressor Scroll /Digital Scroll Compressor		
3	<b>Unit return air temperature</b> : 28 Deg C /40%RH (Scalable to 37 Deg C)		
4	<b>Air Flow Direction</b> : Horizontal-in front of the racks		
5	Cold Aisle Temperature: 22 +/- 1 deg C		
6	Ambient air design température : 45.9 deg		
7	Air Quantity : 80 to 100 CFM/KW.		
8	Humidifier Type: Electronic Controlled Infrared/Immersed Electrode with Electronic Expansion Valve.		
9	Cooling coil should be of copper and aluminium fins and should limit the fan velocity to 2.7 m/s with 5 % tolerance.		
10	Units should be able to work for fixed supply air logic instead of return air control logic. Units should be also connected to cold aisle remote sensors for taking the temperature feedback from the top of the racks at multiple places. This would help to regulate the fan for required airflow in the cold aisles.		
11	Controller: The controls shall be of microprocessor based programmable PID logic controller.		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	Status Report of the latest 400 event-messages of the unit. Input for remote on-off and volt-free contacts for simple remote monitoring of low and high priority alarms: high/low temperature, fan/control failure, compressor/control failure and others are available LAN management: functions provided as standard include stand-by (in case of failure of the unit in operation, the second one starts automatically), and automatic rotation. Automatic restart after a power failure.		
12	There should be provision for integration of the units with Fire Alarm system for tripping of the units during fire emergencies.		
<b>Desired Technical Requirements</b>			
1	SNMP/RS 485 Modbus for integration with DCIM		
2	G 4 Rated Filters		
3	EC fans with outlet velocity of range 7.5 to 8.5 m/s		
4	Dehumidification process should happen by control of Refrigerant through Electronic expansion valve and not by reducing fan speed.		
<b>OEM Qualification Criteria</b>			
1	Manufacturer Authorization letter (As per format) to be submitted along with technical bid.		
2	Must have operational service Centre (Since last 5 years) in Bhubaneswar or within 50KM radius of site. Bidder to provide proof of address of facility in form of GST registration/MOA/Company or firm registration		
3	At least 10 installations of single or multiple units in India for the offered rating. Proof in form of purchase order either in name of Bidder or OEM to be furnished.		
4	The OEM must have been in production, supply, and maintenance of PAC systems at least for 10 years till the submission date of the tender. Proof of facility in form of GST registration/MOA/Company or firm registration or self-declaration signed by head of Production unit.		
5	The OEM must have manufacturing facility in India. Proof of facility in form of GST registration/MOA/Company or firm registration		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	or self-declaration signed by head of Production unit.  Note: Declaration for Sl.3 and 4 can be a single letter.		
6	Both INROW & PERIMETER COOLING SHOULD BE FROM SAME OEM for ease of Execution and maintenance.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	In Row PAC	2	Control of Refrigerant through Electronic Expansion during Dehumidification process	Available	1
				Non Available	0.5
			Air Quantity	>=100 CFM/KW	1
				<100 CFM/KW	0.5

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

## 5.22.4 Precision Air Conditioner (CRAC) for perimeter cooling of Power Rooms

Rating / Sizing: As per Bidder's solution.

Sr. No.	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark
<b>Mandatory Requirements</b>			
1	THE DX TYPE PRECISION UNIT SHALL BE DESIGNED AS PER FOLLOWING CONDITIONS		
2	<b>Unit return air temperature</b> : 27 Deg C /45%RH (Scalable to 37 Deg C)		
3	<b>SHR</b> : Above 0 .92		
4	<b>Compressor:</b> Steeples Capacity Modulation Scroll /Digital Scroll Compressor		
5	<b>Net Sensible Cooling Capacity</b> : As Per Requirement.		
6	<b>Air Flow Direction</b> : For Power Rooms- <b>Bottom frontal discharge-Top return.</b>		
7	<b>False Floor</b> : False floor Height should be more than 600 mm.		
8	<b>Air inlet Temp &amp; RH</b> : Set point $\pm 1^{\circ}\text{C}$ (DB) & Set point $\pm 5\%$ (Return Air)		
9	<b>Air Quantity</b> : As Per Requirement		
10	<b>Quantity</b> : (N+1) Configuration.		
11	<b>Humidifier</b> : Infrared Type		
12	Units should be able to work either on fixed supply air logic or return air control logic. In case of supply air logic, units should be also connected to cold aisle remote sensors for taking the temperature feedback from the top of the racks at multiple places. This would help to regulate the fan for required airflow in the cold aisles.		
13	Refrigerant – R410A		
14	Controller: The controls shall be of microprocessor based programmable PID logic controller. Status Report of the latest 400 event-messages of the unit. Unit memory shall hold the 200 most recent alarms with time and date stamp for each alarm Input for remote on-off and volt-free contacts for simple remote monitoring of low and high priority alarms: high/low temperature, fan/control failure, compressor/control failure and others are available LAN management: functions provided as standard include stand-by (in case of failure of the unit in operation, the		

	second one starts automatically), and automatic rotation. Automatic restart after a power failure.		
15	There should be provision for integration of the units with Fire Alarm system for tripping of the units during fire emergencies.		

**OEM'S QUALIFICATION CRITERIA:**

1. Manufacturer should have experience in manufacturing & installation of Precision AC units in India for last 10 (Ten) years.
2. Installation base of Minimum of 100 units of same model and 20 units in eastern region in India.
3. Fully equipped Service centre at Bhubaneswar running from last 5 years.
4. Software generated output of proposed unit is must.
5. Both INROW & PERIMETER COOLING SHOULD BE FROM SAME OEM.

\*\* Documentary Evidence for all above should be submitted on company letter head along with Relevant proof. Such as Certificate of Registration / Copy of Purchase Orders etc.

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	PAC	2	SHR	$\geq 0.92$	0.5
				$< 0.92$	0.25
			Installation base in India	$\geq 100$	1
				$< 100$	0.5
			Manufacturing experience in India	$\geq 10$ years	0.5
				$< 10$ years	0.25

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

### 5.22.5 Diesel Generator

#### Rating / Sizing: 1800KVA (Data Centre Continuous rated)

##### Product/Solution Description

The existing State Data Centre in OCAC building already had 3 numbers of 380KVA generators in N+1 configuration with an output DG synchronization panel sets installed in the premises. These are feeding the Data Centre dedicatedly.

The new Proposed Diesel generators shall replace the existing Diesel generators. These 2 numbers of 1800KVA Data Centre continuous rated Diesel Generators will feed the existing Data Centre and the new proposed Data Centres. Please refer the layout and SLD for further details

##### Scope of Work

1. Supply of Diesel Generator systems Unloading, shifting, Storing, Installation, Testing and Commissioning
2. Supply of 2 nos. HSD tank of 5 KL each with Unloading, shifting, Storing, Installation, Testing and Commissioning
3. Removal of existing DGs and accessories
4. Supply and installation of Exhaust stack
5. Periodic maintenance
6. SLA adherence
7. Repair and Replacement if required
8. System Acceptance test at Factory and at Site ( on full load condition)

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	The Diesel Generators must be Data Centre continuous rated. This essentially mean supplying power continuously to a constant load for unlimited hours in a Data Centre application		
2	Voltage regulation: Random and no load to full load condition = +/- 1%		
3	Engine Design must be multi cylinder, V block Turbo charged.		
4	Standard engine cooling system by 40 deg C ambient radiator.		
5	Alternator design to be brushless, 4 pole, drip proof revolving type.		
6	Exciter must be PMG type.		
7	AC waveform THDV at no load to be <1.5% and at non distorting balanced linear load to be <5%		
8	Microprocessor based integrated control system providing voltage regulation, engine and		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	Alternator protection, operator interface and Isochronous governing. Synchronisation to be attained through integrated controller only. No external controller allowed. The system must be able to send all the data to DCIM through all possible and acceptable protocols.		
9	Engine should have volumetric capacity of minimum 50 ltr or higher.		
10	The offered PCC controller must have all engine/ alternator protection / synchronizing feature inbuilt inside genset controller.		
11	Underground HSD tank with pumps, piping, digital fuel meter and other accessories including fencing over the platform.		
12	All major performance component of DG sets like Engine, Alternator, Radiator, Battery etc should have the same make only for better coordination, maintenance & manageability.		
13	Warranty of five major components (Crank Shaft, Can shaft, Cylinder head, cylinder block & connecting rod) shall be minimum of 5 Years or 5000 Hours whichever is earlier.		
<b>OEM Qualification Criteria</b>			
1	Manufacturer Authorization letter (As per format) to be submitted along with technical bid. ( Note: Only one OEM allowed)		
2	Must have operational service centre (Since last 5 years) in Bhubaneswar or within 50KM radius of site. Bidder to provide proof of address of facility in form of GST registration/MOA/Company or firm registration		
3	At least 20 installation in India for the offered rating or higher. Proof in form of purchase order either in name of Bidder or OEM to be furnished.		
4	The OEM must have been in production, supply, of Product at least for 10 years till the submission date of the tender. Proof of facility in form of GST registration/MOA/Company or firm registration or self-declaration signed by head of Production unit.		
5	The OEM must have manufacturing facility in India. Proof of facility in form of GST registration/MOA/Company or firm registration or self-declaration signed by head of Production unit.  Note: Declaration for Sl.3 and 4 can be a single letter.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Diesel Generator	2	Engine volumetric capacity	> 50 Litres.	0.8
				=50 Litres.	0.4
			Voltage Regulations	Less than +/- 1 %	0.4
				= +/- 1 %	0.08
			Service Centre in Bhubaneswar	Yes	0.4
				No	0.08
Fuel efficiency@75% load	<275 Ltr per hour	0.4			
	>275 Ltr per hour	0.08			

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

#### 5.22.6 Track Busway system (Continuous)

##### Rating/Sizing: 160A/250A

**Product/Solution Description:** Track Busway System shall be designed primarily for overhead power distribution of electrical power with Continuous Access where the plugin unit/Tap off can be connected anywhere along the busway and which would allow insertion and removal of the plugin units without De-Energizing the busway-Hot swappable. The System should be maintenance free and sections of the bus bar should be joined without the use of Joint packs which need bolting and without the need of torquing, In other words it should be a press fit design to join to sections.

Three-phase Track Busway system with the following features:

- 1 Extruded aluminum busway housing with copper conductors meant for data Centre application
- 2 Power Feed
- 3 Plug-in units for power distribution
- 4 Monitoring
- 5 Installation tool and joint kits
- 6 Optional accessories

**Scope of Work:** The scope of work includes (but not limited to) supply, installation, testing and commissioning of the continuous open channel, low voltage bus bar system in the data centre. Any other consumable items, materials required for civil and electrical works (if any), essentially required to complete the bus bar installation without any extra cost. Spares to be maintained onsite to achieve SLA defined in the RFP.



The Installation shall be carried out in accordance with the drawings and applicable Engineering standards. Any variation or changes to be carried out at site shall be done with prior approval of the End customer

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	System Voltage – 600V Earthing - 100% isolated earth Insulation Voltage -1000V Frequency – 50Hz		
2	Ampacity 160A/250A		
3	Neutral Ampacity should be 200% of the active conductor		
4	KA Rating for 160A / 250A / 630 A should be a minimum of 10KA for 1 sec		
5	If housing is used as ground then it should be 100% PE applicable for Extruded aluminium body only , For others a separate ground has to be considered		
6	Busway shall operate with continuous load with no derating up to 40 degrees Celsius		
7	Relative humidity should be 0 to 95% non-condensing		
8	Busway sections should range from 0.6 Meters to 6 meters		
9	The bus bar conductors shall be continuous copper fabricated from high strength electrical grade Copper (C101 BS 1432/1433) 99.99% Purity to ETP 99.9		
10	End feed should have power monitoring with Temperature sensor		
11	Connection to the End feed unit should using cables		
12	Tap-off Boxes should be capable of inserting safely when bus bar is live.		
<b>Desired Technical Requirements</b>			
1	Plugin Units to be polarized to prevent incorrect installation		
2	Plugin units shall not require any tools to mount it to the busway		
3	Plug-in units shall be configured by the manufacturer to balance the load based on quantity of plug-in unit types provided		
4	The busway shall be installed with the open access channel facing downward, or to the side for special applications. Special installation shall be agreed upon by the manufacturer		
5	End caps will be provided to install at the end of each run		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
6	The closure strip is an optional accessory that can be cut and fitted to cover the bottom opening of the Track Busway housing to prevent dust and debris. Closure Strip can be field modified for fit.		
7	The bus bar should be available with options of colors identification to help differentiate/identification of power source from different power sources.		
<b>OEM Qualification Criteria</b>			
1	A minimum of 15 years' experience in the manufacturing of the Track busway product		
2	At least there should be 5 medium to large installed site in the region with the Track busway system. Bidder to provide proof by submitting copy of work order.		
3	At least 2 Installation with track busway should have been done in a Government establishment		
4	Local presence in India to support along with availability of spares available in India		
4	A reputed 3 <sup>rd</sup> Party certificate such as VDE or UL to be provided to support for live insertion of plugin units in to the busway		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Track Bus way System	1	Polarized Plugin Units	Yes	0.5
				No	0.1
			Installations in India	>5 nos.	0.5
				<5 nos.	0

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

**5.22.7 Sandwich Type Bus duct System**

**Scope of Work:** This specification is intended for design, manufacture, testing, transporting to site of 415V, 3 phase, 50 Hz compact sandwiched type Cu or Al conductor LT Bus Trunking Systems, suitable for Indoor installation.

The equipment shall be of type tested design at CPRI / Independent test house for short circuit, temperature rise and dielectric tests of the ratings required as per SLD & BOQ . Equipment needs to carry ASTA Diamond / KEMA KEUR Certificate which ensures adherence of product quality similar to the one used during type testing by surveillance of manufacturing set up.

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	Ingress protection for the enclosures shall be fire rated as per ISO 834, Indoor Bus Duct Min IP65 (with canopy) and IP54 for tap off.		
2	Expansion joints may be provided as per manufacturer's design and recommendation. The integral earthing shall be of 50% Al run along the length of Bus Duct system incorporating aluminium/ equivalent material which has better thermal conductivity for fast heat dissipation. End covers shall be provided as required. Neutral shall have same cross-section as phases.		
3	Two separately run of Al flat or as specified shall be run externally along the length of the bus duct as earth bus. All parts of the bus enclosure, supporting structures and equipment frames shall be bonded to the ground bus.		
4	Epoxy Coated paint-OEM Standard Specific.		
5	Bus trunking system shall be complete with all accessories like bends, bus duct, expansion joints, flexible connections, and fixing /suspension arrangement etc. to suit site requirements. Type Test Certificates confirming/validating design/performance of these accessories are required for review and approval. Bus trunking systems shall be complete in all respects whether any item is individually listed in schedule of quantities or not.		
6	Installation of the Bus Duct shall be carried out as per manufactures instruction. For Bus Duct horizontal runs, a horizontal expansion units shall be provided at suitable interval as required by design and at expansion joints of the building structure and the system shall be supported at every 1.5m.		

## 5.22.8 MV Panels

**Rating/Sizing: 63A to 6300A****Product/Solution Description**

Unless specified otherwise Main Distribution board / L.V. Panel shall conform in design, material, construction and performance to the latest editions of the International recommendations (IEC standards) and its corresponding British / European standards (BSEN standards) and in particular to the following publication

Low Voltage Switchboard IEC 61439-1/BS EN 60139

Degree of protection IEC 60529.

Over Voltage Category to II

Degree of protection against mechanical impact shall be IK09/10 in

Accordance IEC 62262

Internal arc containment test in accordance to IEC61641

**Scope of Work**

The scope of work for panels may be as follows.

- Supply, erection, installation, factory testing, testing at site, commissioning and integration.
- Removal/shifting of existing panels after disconnection.
- HT panel, Transformer output panel, Main LT panels, DC LT panels and all such panels

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	The main distribution boards shall be of standard, natural air cooled, well tested and proven design which ensures maximum safety to personnel, maximum service reliability and economic operations for a lifetime of at least 20years. Design and construction shall be simple, well laid-out and shall provide good accessibility to components and parts.		
2	Unless specified otherwise, the form of construction for the main distribution board shall comply with Form-4b requirements of IEC 61439-1. And 2		
3	The electrical system for all main distribution boards shall be 415 / 380V, 50		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	Hz 3phase and neutral, 4-wire solidly earthed. The main distribution boards shall be suitable for operating voltage up to 690 V and Insulation voltage of 1000V		
4	Unless specified otherwise, the fault level withstand capacity of the main distribution board bus bar system rated up to 5000Amps shall be 65KA RMS for 1second as minimum standard. The breaking capacity of the switching devices shall be 65KA as minimum standard. The type test certificate shall be submitted for consultant engineer verification, to prove the fault level withstand capacity of the main distribution boards. Even under extreme conditions of short circuit or mal-operation there shall be no danger to persons in the vicinity of the assembly.		
5	All equipment and components of the main distribution boards shall be capable of continuous operation at their full current and voltage ratings and without detriment or malfunction at system continuous deviation of up to and including the following percentages of the normal values.		
6	The enclosure system shall be <b>Modular</b> in nature with <b>Bolt</b> on construction.		
7	Load Bearing members and main Bus bar supports should be from OEM Only		
8	Panels should be tested for mechanical impact as per IEC62262 for IK09 with double door design		
9	Panels should be internal arc tested as per IEC-61641 for 65 KA at 0.3 secs		
10	The enclosure shall be powder coated to an approved colour. The painting process shall include removal of moisture on the sheet steel surface using and applying thermosetting polyester powder using automatic guns. Polymerization of the powder shall take place when the components are cured at about 180°C,		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	forming a continuous integrated coating. A fairly uniform coating of at least 70-80 microns shall be provided.		
11	All incomer lines and major outgoing lines must have multifunction meter that measures all the parameters including harmonics till 15 level. Such incomers and outgoing lines must have indications for phases and On,OFF, TRIP, breaker control switch etc.		
<b>Desired Technical Requirements</b>			
1	The pre-treated and powder coated sheet steel components shall be at least tested randomly at regular intervals for coating thickness measurement, adhesion test, bend test, impact test, hardness test, salt spray test etc.		
2	Main distribution board enclosure shall be fabricated of minimum <b>1.5mm</b> thick electro-galvanized sheet steel folded construction. The enclosure shall be of simple and robust construction designed for a variety of dimensions obtainable by means of standardized basic elements. Main distribution board shall consist of several enclosures of equal height and depth mounted side by side to form a composite board of uniform assembly.		
3	Unless specified otherwise, Main distribution boards shall be designed for front access for the purpose of operation and access to all components and shall suit front or rear access for cable connections and top or bottom for cable entries. Wherever required, enclosure shall be suitable for bus duct entry at the top. The access and entries shall be provided as per site requirements.		
4	Enclosure shall be readily suitable for future extension on either side without any modifications (after installation at site).		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
5	The bus bar system shall be designed as per the pre-defined guidelines provided by the original manufacturer. The bus bar system shall be type tested by the manufacturer at reputed laboratory for short circuit withstand capacity. The neutral and earth bus bars shall also be type tested for the short circuit withstand capacity. The fault level rating of the bus bar system shall be as per the drawings however the minimum short circuit withstand capacity shall be 50KA RMS for 1second. Neutral bus bar shall be able to withstand a thermal stress of at least 50%, corresponding to the main phase bus bar rated short circuit withstand capacity.		
6	The bus bars shall be high grade electrolytic tin plated copper (with 99.9% conductivity), rectangular and rigid construction. The phase bus bars and neutral bus bars shall be arranged systematically in a bus bar chamber/ alley. The bus bars shall be colour sleeved throughout the length for phase identification (except for the distribution bus bars of the withdrawable sections). The bus bars shall be shrouded completely using metallic partitions and/or polycarbonate shrouds as applicable. The bus bar assembly shall be shrouded (at least IP20) by shrouds so that no live parts are accessible. Phase identification shall be done systematically. Use of Bakelite sheets for shrouding will not be permitted.		
7	Distance between the bus bar supports for bus bar system and the distance between different phases of bus bar system shall be as per manufacturer guidelines based on the type test results.		
<b>OEM Qualification Criteria</b>			
1	Panels must be CPRI type tested		
2	The OEM (panel manufacturer) must have local service centre in Bhubaneswar		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
3	Panels and Breakers from the same OEM		
4	At least 20 installations of From 4b panels in India. Bidder has to get a self-declaration from OEM in their letter head.		
5	At least 5 installations of more than 500A from 4b panels in Eastern region. Proof must be submitted.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	MV Panels	0.5	Installation of similar From 4b panels in eastern region. Documentary evidence required	>5 Installations	0.25
				<=5 Installations	0.125
			Service Centre at Bhubaneswar	Available	0.25
				Not Available	0.125

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

## 5.22.9 Passive networking

**Rating/Sizing: Fiber and Copper 10G/40G****Product/Solution Description**

**The Data Centre network cabling will be over the racks through cable basket for Copper and Fiber pathways. Each Row will have End of the Row network rack. Every Rack will have 12+12 fiber ports in redundant mode and similarly 6+6 copper ports as well. The cabling standard will be as per TIA-568B or its latest amendments. Tier-3 architecture must be followed for the cabling.**



**Scope of Work**

**Supply, installation, testing and commissioning of network cabling system Including cables, Cable basket, Fiber Runner/Pathways, jack panel/patch panel/ MPO cassettes/Patch cords etc and Maintenance of the same for the contract period.**

- The structured cabling for data Centre shall cover Copper & fiber optic cabling for all racks within the DC hall, backbone up to Network rooms/racks, and backbone up to ISP racks.
- Adequate redundancy need to be planned in the cabling design as per requirement to minimize failures.
- The proposed cabling system should support at least 10G on Copper and up to 40G / 100G on fiber.
- The fiber cabling should be modular (plug-n-play) in nature using MPO trunks and connectors and be scalable from 40G to 100G.
- For all backbone cabling, splicing based terminations for fiber could be used as per design requirement.
- Minimum of 2 Mux rooms/POE rooms need to be provisioned with a separation of at least 20 mtr. Each Mux room shall connect to the DC Core network over fiber and copper cabling.
- Adequate Copper LAN cabling to be considered for DC support areas and other functional areas as required.
- All terminations and testing shall be performed in compliance with the TIA 568-C and ISO/IEC 11801 requirements.
- Dedicated copper trays and enclosed fiber pathway system to be considered for respective cable routing for the entire Data Centre.
- The cable pathway design must consider the cable fill ratio, separation and bend limits as per TIA 569-C, ISO/IEC 14763-2:2012 and BICSI TDMM 13 design guidelines.

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>A</b>	<b>Architecture and General Construction</b>		
1	The system shall utilize MPO-compatible 12-fiber / 24-fiber male and female connector		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	plugs that are compatible with MPO adapters per IEC 61754-7 and TIA 604-5.		
2	The system shall utilize “aligned key” adapters for every MPO mated connection, per TIA 604-5, K=2.		
3	The system shall guarantee correct Transmit/Receive polarity in any configuration or combination of system components.		
4	The system shall allow for the use of TIA compliant patch cords and trunk cables on both ends of every link, for both duplex and full-parallel applications.		
5	The system should support Fibre Performance calculators available at OEM website for verification of the designed fibre links against a given set of applications.		
6	The system shall support 50/125 Laser Optimized Multimode – available in OM4 and OM5 (Wide Band Multimode)		
7	The proposed system should have been installed successfully in at least 3 data centres in India, in the last 2 years.		
<b>B</b>	<b>Pre-Terminated MPO Modules</b>		
1	LC Modules – 12-fiber or 24-fiber – Shall be available in 50 micron laser optimized OM4 and latest OM5 versions.		
2	The 12-fiber MPO male/female module shall have 6 pre-installed duplex LC adapters at the front routed to a pre-installed 12-fiber MPO “aligned-key” adapter at the back.		
3	The 24-fiber MPO male/female module shall have 12 pre-installed duplex LC adapters at the front routed to 2 pre-installed 12-fiber MPO “aligned-key” adapters at the back.		
4	Cassettes shall have wiring pattern to enable use of same cassette on either end of link, for easy management and scalability or The cassettes (modules) should be one end polarity A and other end polarity B, for matching of link.		
5	The cassettes shall be UL listed. Insertion Loss (MPO): <0.5 dB		
6	The vendor shall provide the application support guidelines for the system		
7	The vendor shall have proven track record of public demonstration of 40/100G.		
<b>C</b>	<b>Modular Panels and Shelves</b>		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
1	The 1U / 2U /4U shelf shall be equipped with a front trough and door for patch cord management and port labelling. Trough door should have clear view of the ports and labels inside.		
2	The 1U panel shelf shall house any combination of up to 4 pre-terminated modules to achieve up to 96 fibre terminations per rack unit at a minimum. To be used in low density server rack end.		
3	The 2U/4U high density shelf shall support up to 144 duplex LC ports to be used in Network racks / SAN racks.		
4	1U / 2U /4U shelves shall have 1/2 stage slide out feature in the front for better inside access.		
5	Shelf shall support both side and rear entry of cables / trunk cords.		
<b>D</b>	<b>Pre-terminated Fiber Trunk Cable assemblies</b>		
1	All cables shall be constructed with one or more subunits, each with 12 fibers surrounded by a jacket containing aramid yarn strength members.		
2	All cables should be Bend insensitive multimode OM4 or OM5.		
3	The trunk cables shall be available in 12 / 24 fibers with MPO male/female connectors on either end.		
4	The Trunk cable shall have Method B enhanced construction		
5	The cable should have been tested for 40/100G		
6	Trunk Cable dia. Not more than 5.7 +/- 0.2 mm. LSZH jacket with IEC 60332-3 compliance.		
7	Trunk Cables shall have Flame Test Listing of NEC OFNR-LS (ETL) and c(ETL)		
8	LC-LC OM4 / OM5 Patch cords shall be with Uni-boot construction for ease of access in high density panel ports.		
9	Uni-boot patch cords shall support field adjustable polarity reversal, without cord damage.		
10	The vendor should provide the application support table for the trunk and the associated system components.		
<b>E</b>	<b>Horizontal Cable – CAT6A UTP Cable –</b>		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
1	The Cable should be 4 pair 23 AWG solid copper conductor and meet ANSI/TIA 568C.2 Category 6A Specifications and ETL verified.		
2	The cable shall be available in Low-Smoke, Zero Halogen (LSZH) compatibility and The LSZH version must comply with the following Fire Safety standards: 1) ISO/IEC 60332-3-22: Vertical Flame Spread 2) ISO/IEC 60754-2: Acidity 3) ISO/IEC 61034-2: Smoke Density		
3	NEXT - Minimum 3 db above the standards; Should support a minimum of 4 connector Channel with a minimum 3 db guaranteed NEXT.		
4	Cable must be compliance to ANSI/TIA 568-C.2 requirement for both long channel (100m) and short channel (15m) tests. Reports for both tests to be submitted.		
5	The cable and cordage shall be "True UTP" components that do not include internal or external shields, screened components or drain wires. No Special Grounding requirements. The horizontal data cables shall be of shielded twisted pair cordage with eight (8) solid conductors formed into four individually twisted pairs		
6	The horizontal cable shall have a unique print string on the cable jacket to access to a full set of OEM factory tests available publicly for anytime verification by client.		
<b>F</b>	<b>Requirement for CAT 6A Patch Panel</b>		
1	The ganged adapters shall have RJ45 jack in the front and Insulation Displacement Connector (IDC) at the rear of the module.		
2	Termination managers must be provided with panel to provide proper pair positioning, control, and strain relief features to the rear termination area of the panel.		
3	3rd Party Verification test certificates shall be provided to show compliance to ISO/IEC 11801 Amendment 2 testing for Cat 6A components.		
4	The panel shall be equipped with removable rear mounted cable bundle managers.		
5	Insertion Life = 750 minimum insertions of an FCC 8-Position Telecommunications Plug		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>G</b>	<b>Requirement for CAT 6A LSZH U/UTP RJ45 Patch Cords-</b>		
1	CAT6A Patch Cords shall constructed of 23 AWG solid core copper and equipped with 8-pin modular plugs on each end.		
2	All cords shall be round, and consist of copper conductors, tightly twisted into individual pairs.		
3	Nominal cordage diameter shall not exceed 7.24 mm.		
4	Plugs shall be designed with an anti-snap latch to facilitate easy removal during move, add and change processes.		
5	LSZH jacket must comply with the following Fire Safety standards: ISO/IEC 60332-3-22: Vertical Flame Spread ISO/IEC 60754-2: Acidity ISO/IEC 61034-2: Smoke Density		
6	The cordage shall be UTP components that do not include internal or external shields, screened components or drain wires.		
7	The patch cords will have insertion life of 750 cycles minimum.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Passive Cabling	0.5	The complete solution should be intelligent ready from day 1 of installation.	Yes	0.25
				No	0
			Installation of similar products in at least 5 Data Centres (minimum 1000 copper + Fiber ports) across India in last 2 years. Documentary evidence to be submitted.	>=5 Data Centre with minimum 1000 copper + fiber ports in last 2 years	0.25
				1-4 Data Centre with minimum 1000 copper + fiber ports in last 2 years	0

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

5.22.10 DCIM

**Rating/Sizing: As per bidder’s solution**

<p><b>Product/Solution Description</b></p> <p><b>Data Centre Infrastructure Management (DCIM) Solution tool has to integrate all possible Non IT and IT field devices into one platform for effective monitoring of Data Centre operation.</b></p>
<p><b>Scope of Work</b></p> <p><b>Supply of all end to end hardware and software, Installation, testing and commissioning Maintenance for 5 years including product/solution upgrades, patch updating, etc</b></p>

Sr. No.	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark
<b>Mandatory Requirements</b>			
1	The proposed 100% web based DCIM should have following modules: a) Inventory Manager b) Change planner c) Thermal Systems Manager d) Site Manager e) Power System Manager f) Energy Insight		
2	Proposed DCIM should have a single platform with combination of application server and database server with data collection engine.		
3	The solution should have symbols library more than 10,000 vendor-neutral symbols. All managed device symbols must include physical dimensions, rated capacities, consumption of space, power and cooling and any other associated manufacturer’s data		
4	Proposed DCIM solution should support complex business process mapping based on requirement. Example: - commission, de-commission, add and modify.		
5	Thermal heat map - should visualize thermal data in the form of heat maps in a 3D rendering of the floor view.		

Sr. No.	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark
	And should allow to view actual rack heat load and to help balancing and optimizing the system and generate reports		
6	DCIM should have capability to customize dashboard as per customer requirement.		
7	Dynamic Single Line diagram should enable logical mapping from LT/ HT Panel to IT equipment and provide exact alert/alarm can be pin point problems through this solution.		
8	The solution shall support all levels of role based access control and fine grain authorization for each functional department		
9	Proposed DCIM should be able to integrate with third party BMS solution (to integrate OSDC 1.0 or any other existing BMS tools).		
10	Space, power and cooling capacity management: End to End DC facility view to analyse data such as rack capacity, maximum rack space available, weight, and available space in racks/dc floor to improve capacity.		
11	Proposed DCIM should have Map view to have high level understanding on multi-location Data Centres		
12	DC design capability: Upload floor plan images and utilize drag-and-drop functionality to place equipment within the floor plan including detailed rack elevations with rack load, space utilization, relationship rules and inventory monitoring built in.		
13	At minimum DCIM should provide these reports (hourly, daily, weekly, monthly, quarterly, yearly): Availability/Reachability Report, Total UPS load, Used UPS load, Total cooling capacity, Used cooling capacity, Total/Used/Available U-space (floor level & at rack level), Ambient and Inlet temperature, Energy Efficiency PUE/DCiE trend, rack level power consumption report, Alarm reports, quick access to information such as current capacity, asset lists and exact device location.		

Sr. No.	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark
14	The solution provides alert compression and advanced alerting algorithms including deviation from normal and time over threshold to help reduce false positive alarms.		
15	The solution will provide provisions to recommend the best location for a server in the rack layout, utilizing available space, cooling, and power capacity to optimize capacity utilization.		
<b>Desired Requirements</b>			
1	Proposed DCIM shall provide mobile device capability preferably iOS solution. It shall enable barcode and device recognition for easy inventory management. It shall include an audit capability, so user can scan and asset and quickly determine correct or incorrect placement of the device.		
2	Proposed DCIM solution should have capability to provide console management of Virtual and Physical servers and serial devices.		
<b>OEM Qualification Criteria</b>			
1	At least 5 installations in the country. Documentary proof required.		
2	OEM should have a service centre in Bhubaneswar with local GSTN.		
3	The proposed DCIM should be from the leader quadrant of the Gartner Report and IDC research report of year 2016 or above.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	DCIM	0.5	No. of implementations in PSUs/PSBs/ Government organizations	>5	0.25
				Between 3 to 5	0.1
			User Defined Reports and Dashboard	Yes	0.25
				No (Fixed Dashboard)	0

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.



## 5.22.11 Asset Tracking

**Rating/Sizing: As per bidder's solution**

<b>Product/Solution Description</b>
<b>Asset tracking tool is to manage the entire asset of the Data Centre.</b>
<b>Scope of Work</b>
<b>Supply of all end to end hardware and software, Installation, testing and commissioning Maintenance for 5 years including product/solution upgrades, patch updating, etc</b>

Sr.No	Requirement: Asset Tracking	Description	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark
<b>Mandatory Requirement</b>				
1	Objective	Rack level IT Asset Tracking to optimize and automate Datacentre IT inventory Tracking and audits.		
2	General Functionality	Solution should be able to collect the information of IT assets and upload to a central software. Near Real time monitor the assets location up to rack level, notify the user if a asset is added, moved, removed		
3	Communication	Solution proposed should be wireless in nature.		
4	Frequency	Wi-Fi frequency used by solution should not interfere with WIFI Network within data center		
5	Asset Tag form factor & mounting	Form factor of asset tags should be small enough to be able to easily attach to a IT asset but it should also be noticeable to naked eye, important is no cables and wiring should run between asset tag & any other hardware or controllers or gateways, thus avoiding complexity, unnecessary cable logging inside or side of rack, such cabling block airflow & also obstruct service of IT equipment's.		
6	Asset tag battery Life	Asset tag must have a battery life to work uninterrupted for minimum of 5 Years from date of installation & commission		
7	Asset tag integrity	Should be able to alert if asset fall, forceful removal of tag from asset,		

		low battery, asset is moved from room		
8	Alarms & Notification	Solution should be able to provide real Time alarm & event notification. Should be able to Generate Alert in following conditions: 1. Addition / removal of Asset 2. Unauthorized move of Asset Alarm 3. Out-of Warranty Alarm		
9	Local Indicator	All tags should have in-built indicators to reflect working status		
10	Data Integration	proposed solution should be able to route the data to DCIM by forwarding SNMP traps across SNMP v1 & SNMP v3		
11	Protocols support	Support HTTP, HTTPs, SSH, SMTP, FTP, SNMP v1, SNMP v3, MQTT		
12	Data Security	Support encryption to ensure effective access control and integrity for SSL browser and SSH session		
13	Security	1. must supports TSL & SSL. 2. adheres to FIPS - Level 3. access is protected through username & password. 4. Tampering such as any forced actions are detected and logged		
14	Environmental Certification	Certification: RoHS, CE		
<b>Desired Requirement</b>				
1	Capability	Locate IT asset accurately to a distance of +/- 80 cm / Rack Level Accuracy		
2	Operational Life	Asset tags Battery must also be replaceable in nature		
3	Scalability	System should support minimum of 5000 tags in an area of 30,000 sqft		
4	Firmware upgrade	Solution should support OTA (Over the Air) upgrade of its components		
5	Data Storage & Operational use	1. Minimum 3 Years of data storage 2. Tag/ readers should have a 2D barcode for ease of configuration 3. If an instruction is given to system to find an asset, it should be possible to locate that asset and give a beep sound locally on tag		
<b>OEM Qualification</b>				
1	OEM	OEM should have a minimum turnover of Rs. 500 cr for the last three years.		
2	Local Service	OEM should have a service center in Bhubaneswar with local GSTN.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Asset Tracking	1	Level of Asset tracking	(Rack level + Room Level) + U Level	0.5
			No of installations	>=5	0.5
				<5	0.2

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

## 5.22.12 IT Rack

<p><b>Product/Solution Description</b></p> <p><b>Server Racks of 42U and 600 mm width x 1200 mm depth and Network Racks of 42U and 800mm width x 1200mm depth for the Data Centre area.</b></p>
<p><b>Scope of Work</b></p> <p><b>Supply, unloading, storing, shifting, installation, testing and commissioning Maintenance for 5 years.</b></p>

Sr. No.	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark
<b>Mandatory Requirements</b>			
1	42U Server and network rack dimension would be (WDH) 800mmX1200mmX 2000mm respectively.		
2	RAL7021 Black powder coat on all sheet metal components of the rack.		
3	All components should be self-grounded. Not wire connection among or to the frame except the doors.		
4	Single front and split rear doors should be min 63% hexagonal perforated (As per TIA 942)		
5	The front and rear doors should open a minimum of 140 degrees to allow easy access to the interior.		
6	Two set of EIA rail should be fully depth adjustable within 980mm use space area.		
7	Two number of Cable manager with full height, multiple standard hole pattern for tool less accessories mounting should be part of the rack. They should have capability to hold two Rack PDUs each.		
8	Rack frame shall support 1200kg static weight load, 1022kg dynamic (non- transit) weight load.		
9	Side panels should be split type with single locking slam latch.		
10	The roof of the racks should be removable from the interior of the enclosure without tools and should		

	have cable entry holes to allow up to 1800 cables or 60A PDU plugs		
11	The racks should be UL Approved and comply to EIA-310, REACH and RoHS.		
12	Minimum 20 nos. of tool-less blanking panels to avoid air recirculation		
<b>Desired Requirements</b>			
1	Racks should have a provision for cable entry from the top and bottom		
2	Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools. The front door of unit should be reversible so that it may open from either side.		
3	The racks should have a minimum of IP 20 rating for protection against touch, ingress of foreign bodies, and ingress of water		
4	19" Rails should accept tool less Cable Management Accessories.		
<b>OEM Qualification Criteria</b>			
1	At least 15 installations in the country. Documentary proof required.		
2	OEM should have a service Centre in Bhubaneswar with local GSTN.		
3	Manufacturing facility in India.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	IT Racks	1.5	Load Bearing capacity (High Density)	>1200 Kgs	0.75
			Rack Perforation level	>75%	0.75
				63-75%	0.375

**NB: Supply of 2 Nos of additional network racks for Telecom Room will be in the scope of the bidder.**

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

## 5.22.13 IPDU

Sr. No.	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark
<b>Mandatory Requirements</b>			
1	Each rack should have two IPDUs with different chassis color for source identification, and each IPDU should support the load from 4kW to 11kW.		
2	Each IPDU should be able to take input from single phase source or three phase sources based on the site load requirement, this will help to reduce the SKU count and have better inventory management.		
3	Intelligent PDU should have min. 30 numbers of hybrid outlets which can be utilized as either C13 or C19 outlet. All outlets should provide high retention to avoid accidental dislodging of power cords.		
4	<p>Monitoring parameters – The IPDU should have monitoring capability at the Strip level, phase level, outlet/socket level monitoring</p> <p>Following monitoring parameters should be included phase and the outlet level.</p> <ol style="list-style-type: none"> <li>1.) Voltage (V)</li> <li>2.) Current (A)</li> <li>3.) Power factor</li> <li>4.) Active power (W/KW)</li> <li>5.) Apparent power (VA/KVA)</li> <li>6.) Energy consumption (Kwh)</li> </ol> <p>The metering accuracy should be +/- 1% compliant to ANSI C12.1 and IEC 62053-21 at 1% Accuracy Class Requirements for outlet/socket, strip and phase level.</p>		
5	Each IPDU must have circuit breakers to protect the PDU and IT devices form damage caused by overload or short circuits. PDU must have 16Amp circuit breakers as per the IEC guidelines.		
6	The iPDU should have color coded and alternate Phase outlets for simplified circuit and phase balancing, reducing cable runs for better airflow management.		
7	It should support High Operating temperature of 0 to 60 deg C to take care of high operating temperature at back of Rack		
8	The IPDU should have 2 nos. of gigabit Network Ports. IPDU should support		

	communication protocols including DHCP, HTTP, HTTPS, Ipv4, Ipv6, LDAP, NTP, RADIUS, RSTP, SSH, SMTP, SSL, SNMP (v1, v2, v3), Syslog and TACACS+. Communication module should be hot-swappable, so that it can be replaced without powering off the PDU.		
9	PDU should support configuration of user defined thresholds, reports and email alerts and send it automatically to the configured users automatically on the scheduled time intervals.		
10	The IPDU should support grouping of minimum 40 rPDU and rPDU sensor in the interconnected array to create the aggregated measurements like total rack power, average temperature, average humidity etc.		
11	IPDU should have separate reset buttons for reset to factory defaults and separate button to reset IP only, if other configurations are not to be altered.		
12	IPDU should have USB support for firmware upgrade, backup, restored device configuration or expand logging capacity via USB storage device.		
13	IPDU should have LED indicators for each outlet and shall have different colors to show the state of the outlet		
14	Each rack should have one sensor in the front of the rack to monitor temperature, humidity, dew point & air-flow and one sensor in the rear to have temperature monitoring.		
15	The IPDU should have approvals from CE, RoHS and UL.		
16	The IPDU input cable should have approvals from IEC, CE, EN and UL		
<b>Desired Requirements</b>			
1	PDU should support Android or iOS app for easy and secure read of full power readings and should not use Bluetooth or Wi-Fi to prevent breach and should not have any additional license requirement.		
2	Sockets should be preferably coloured to clearly identify different circuits.		
<b>OEM Qualification Criteria</b>			
1	OEM should have a service centre in Bhubaneswar with local GSTIN.		
2	OEM should have a minimum turnover of 500 crores for the last three years.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	IPDU	1.5	No. of iPDUs that can be cascaded / IP Aggregation (resulting in savings of Copper Ports)	>=40	0.75
			Environmental Sensor Integration	Temp. + Humidity + Dew point + Airflow	0.75
				Temp. + Humidity	0.375
				No	0

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature

## 5.22.14 Rack Access Control

Sr. No.	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark
<b>Mandatory Requirements</b>			
1	Mechatronic Lock for rack level access control to keep data secure, monitor & audit for server/network racks distributed across different rooms and/or buildings in Data Centre		
2	The lock should be accessible remotely over network with Admin Suite Software and communication via TCP/IP Protocol.		
3	Swing handle lock should have an in build keypad integration for two factor authentications at rack level		
4	Swing handle lock should eliminate the use of mechanical key override to avoid misuse at rack level.		
5	Swing handle lock should have an inbuilt memory storage capacity 2000 employee access cards and pins, 500 events and 30 time profiles to grant and/or restrict access during network or power failure condition		
6	Admin Software should provide complete documentation of all events and overview to enhance security		
7	Four – eye principle for higher security levels for server/network racks in Data Centre		



8	Swing handle lock should have an LED indication for lock status and inbuilt temperature sensor for emergency opening		
9	Admin Software should be server – client based application with encrypted data communication between mechatronic lock, server and client		
<b>Desired Requirements</b>			
1	Swing handle lock should have an in build RFID antenna to authenticate the employee access cards		
2	Admin Software should have AD integration and easy interfaces with 3 <sup>rd</sup> party system		
3	Admin Software should be capable of automated task management with pre-defined reports periodically		
<b>OEM Qualification Criteria</b>			
1	OEM should have a service Centre in Bhubaneswar with local GSTIN.		
2	Manufacturing base in India for the product.		
3	Rack Access Control should be implemented in at least one PSU/Government of India entity with more than 200 racks.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Critical Rack Access Control	1	Capability of Fire Emergency Lockout	Yes	0.5
			Secure event Logging in case of Power Failure	Yes	0.5
				No	0

**N.B : Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

## 5.22.15 33KV VCB Panels (HT Panel)

**Rating/Sizing:** As per bidder's solution

**Product/Solution Description**

The existing 33KV HT panels (one incomer and two outgoing) needs to be replaced with New set of panels.

**Scope of Work**

Supply, Unloading, Storing, shifting, Installation, testing, commissioning after decommissioning and removal of existing panels.

Maintenance for 5 years.

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	Self-supported Bus-Bars to ensure that there are no support insulators required, thereby ensuring longer life, and eventually no Phase-Earth tracking in the Busbar chamber.		
2	Full Voltage Sleeve on the Bus-Bars.		
3	Short Time Current Rating of 31.5kA/3sec and Current rating up to 3150Amps.		
4	Internal Arc: AFLR 31.5kA/1sec. AFLR for full 1 sec		
6	Numerical relay supports IEC 61850 Edition 1 and Edition 2(with test reports) and supports HSR and PRP redundancy protocols.		
7	The IED (Numerical relay) Complies to 61850 protocol without any external protocol converter. GOOSE signals are freely configurable. WEB HMI feature		
8	The panel should have inbuilt heater element for dehumidification purpose during rainy/humid condition.		
<b>Desired Technical Requirements</b>			
1	Making type Earth Switch. Making type Earth Switch eliminates the need of keeping a separate ETCB to be kept and stored at site and ensures operator ease w.r.t maintenance works.		
2	Vacuum Interrupter, Numerical Relay, Circuit Breaker and Panel are of same		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	make as OEM. Ensures excellent overall quality control over all products and ownership by a single vendor in the event of any malfunction / manufacturing defects etc.		
3	Motorized Rack-in Mechanism. Motorized Rack-in mechanism ensures the substation can be truly unmanned since no physical action is required to put the Breaker in Test/Service Position .The operation can be done from SCADA Room remotely.		
4	Wireless Temperature Monitoring and hook up to DCS. Battery less/Wireless Integrated Temperature Monitoring sensors provide Condition monitoring of the Switchgear and helps in taking proactive action for any Switchgear maintenance.		
<b>OEM Qualification Criteria</b>			
1	Manufacturing facility in India		
2	At least 10 installation In India		
3	Local Service Centre at Bhubaneswar		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	HT Panels	1	Service centre in Bhubaneswar	Yes	0.25
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.25
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

5.22.16 Dry Type Transformers

**Rating/Sizing: 3 MVA dry type 33/.433**

**Product/Solution Description**

The equipment will be designed, manufactured and tested in compliance with the IEC, IS and ISO codes and standards and the following codes and standards in particular:

- IEC 60076-11 Dry type power transformers
- IEC 60905. Loading guide for dry type power transformers
- IEC 60076 Series: Power transformers
- CENELEC HD 538 Three phase dry type distribution transformers
- IS 2026 Power Transformers
- IS 11171 Dry type transformers
- ISO 9001

**Scope of Work:**

Supply, Unloading, Storing, shifting, Installation, testing, commissioning after decommissioning and removal of existing transformer

Redoing the Foundation.

Maintenance for 5 years.

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	The transformer shall be designed so that they can deliver continuously its rated current under steady loading conditions without exceeding the temperature rise, assuming that the applied voltage is equal to the rated voltage and that the supply is at rated frequency.		
2	Dry type AN cooled transformers, can be overloaded according to IEC 60905 Loading guide for dry type transformers		
3	The core shall be constructed of the best quality, low loss, cold rolled, grain oriented steel laminations insulated on both sides.		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	<p>Laminations shall be “step lap” overlapped to minimize core losses and noise.</p> <p>The entire core assembly shall be covered with heat retardant resin-based lacquer for corrosion protection before the coils are mounted</p>		
4	<p>All the windings shall be of high conductivity conductors of best quality. The transformer shall have separate high voltage and low voltage windings. The insulation system of the windings shall consist of approved materials for assigned temperature class.</p>		
5	<p>The Fire, Environmental, and Climatic classes should be as stated below:</p> <p>Environmental Class: It shall be E2 in order to be able to withstand condensation or pollution or combination of both.</p> <p>Climatic Class: It should be C1 or C2:</p> <p>C1: Indoor installation. The transformer is suitable for operation at ambient temperatures not below – 5 deg C, but may be exposed during transport and storage to ambient temperatures down to – 25 deg C.</p> <p>C2: Outdoor installation. The transformer is suitable for operation, transport and storage at ambient temperatures down to – 25 deg C.</p> <p>Fire Class: It shall be F1. Transformer subjected to fire hazard. Restricted flammability is required. Self-extinction of fire (poor burning is permitted with negligible energy consumption) shall take place within a specified time period to be agreed between purchaser and manufacturer, unless specified by National Specification. The emission of toxic substances and opaque smokes shall be minimized. Materials and products of combustion shall be practically halogen-free and shall contribute with a limited quantity of thermal energy to an external fire.</p>		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
6	<p>HV windings shall be vacuum cast with aluminium disk foil as conductor material and 180°C (class H) insulation system temperature (copper foil can be also accepted).</p> <p>Winding design shall be adequate to allow for full encapsulation with filled resin under vacuum. The resin system shall be two components epoxy filled with a mixture of inorganic fillers improving its thermal, mechanical and fire behaviour properties. The single resin components and filler will be carefully stirred and degassed under vacuum in order to eliminate all air bubbles and then mixed together throughout a static mixer just before to pour them, under vacuum, into the mould that contains the coil (winding). The position of this mould shall be horizontal during the casting process that shall assure the total elimination of air bubbles that could create air cavities and critical points of partial discharges.</p> <p>The surface of the encapsulated winding shall be smooth and completely closed and impervious to moisture and common industrial contaminants</p>		
7	<p><b>High Voltage Connections</b></p> <p>The HV cable terminals will be made in copper / aluminium material, located above the top of the connection bars.</p> <p>Each terminal will be drilled with a 13 mm hole ready for connection of cables.</p> <p>The HV delta connection will be made through copper bars protected by heat shrinkable tubing and flexible cables.</p>		
8	<p><b>Low Voltage Windings</b></p> <p>The LV windings will be of non-encapsulated design with aluminium foil wound (copper foil can also be accepted) together with an insulating pre-impregnated B-stage epoxy resin and thermally cured in an oven to achieve thermal, mechanical and moisture penetration properties that are comparable, for LV coils, with those of cast windings.</p>		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	In high polluted or aggressive environments it is recommended to seal both edges (top and bottom), that will prevent the entry of dust or moisture inside the coil.		
9	<b>LV connections</b> The LV connections will be made from above onto bars located at the top of the coils on the opposite side to the HV connections. All the terminal connection bus bars shall have half round edges.		
10	<b>Short – Circuit Withstanding</b> The transformer shall be capable of withstanding, on any tapping, for two seconds (IEC value = 2 s), without damage, under service conditions, the thermal and mechanical effects of a short – circuit at the terminals of any winding.		
<b>Desired Technical Requirements</b>			
1	<b>Thermal insulation class</b> The insulation system temperature for HV and LV winding will be 180°C (class H).The average winding temperature rise for both HV (at rated tapping position) and LV windings at full load shall not exceed 115°C (class H) (over an ambient temperature equal to 50 deg C)		
2	<b>Off circuit tapping</b> The transformer shall be provided with tapping links on the HV windings. Their position can be selected whilst the transformer is off circuit. Taping selection shall be by means of bolted links. The tapping range shall be: <ul style="list-style-type: none"> <li>▪ Plus 2.5% and 5%</li> <li>▪ Minus 2.5% and 5%</li> </ul> Tapping with connection cables are not accepted.		
3	<b>HV and LV windings assembly</b> The high and low voltage coils of each phase shall be supported and clamped by lower and upper supporting blocks, each having rubber expansion blocks for thermal expansion.		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	<p>The position of the LV terminals shall be either at the opposite side of the HV terminals at the top or at the bottom of the transformer. The neutral bar terminal, if any, shall be at the same side as the LV phase terminal.</p> <p>The design of the complete assembly should be in a way that if necessary, an exchange of separate high and low voltage coils can be done.</p>		
4	<p><b>Noise level</b> Noise level shall be in accordance to the NEMA TR 1 / CENELEC standards.</p>		
5	<p><b>Earthing terminal</b> Provision shall be made to connect external earthing at position close to the bottom the enclosure at two points. Earthing terminal shall be adequately dimensioned to receive the external earthing conductor/strip.</p>		
6	<p><b>Internal earthing arrangement</b> All metal parts of the transformer with the exception of the individual core laminations and associated individual clamping plates shall be maintained at some fixed potential. The bottom main core clamping structure shall be connected to the enclosure by copper cable.</p>		
7	<p><b>Standard enclosure</b> The enclosure is made of bolt-on type sheets of steel of the bolt-on type with removable panels and supported from the transformer framework. Its removable base can be installed without having to lift the transformer.</p> <p>Central front and rear handle panels will be provided for access to the tap changer.</p> <p>Inlet-outlet of cables is situated at the bottom of the enclosure through aluminium gland plates to be machined by the customer.</p> <p>For indoor applications the sheet steel will be painted in grey color, RAL7035 with average 70 µm powder coating thickness ; for outdoors applications will be will be painted in grey color, RAL7035 with average 100 µm powder coating thickness.</p>		



Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>OEM Qualification Criteria</b>			
1	Manufacturing facility in India		
2	At least 10 installation In India		
3	Local Service Centre at Bhubaneswar		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Transformer	1	On load tap changer (OLTC) and remote tap Change control (R.T.C.C.) panel	Yes	0.25
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.25
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

5.22.17 Fire Detection & Alarm System

**Sizing: As per bidder’s solution**

**Product/Solution Description**

Addressable fire detection system will be implemented all across the Data Centre and support area. The integration of Fire system has to be with DCIM and other critical equipment.

**Scope of Work**

Supply, Installation, testing and Commissioning of Fire detection and alarm system  
 Maintenance of the same for 5 years  
 Integration with Building fire panel and DCIM  
 Integration with Access Doors and PAC

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	2 loop panel with LCD display, Per loop 250 Devices handling capacity of any combination, power supply and battery backup. If require Each Loop shall be able to configure in two physical loop.		
2	The fire alarm system shall be integrated with the access control system to deactivate all door locks in case of emergency.		
3	Instructions/signal from panel should also shut down the PACs in case of fire.		
4	The fire alarm system should also be integrated with the BMS through SNMP CARD/Modbus/BACnet interface to get all the alerts and alarm on the BMS		
5	Each Loop with 250 device capacity capable to handle the following detectors and devices.		
6	Analogue Addressable Photo type Smoke Detector with Detector base Server Farm Area		
7	Analogue Addressable Multi Criteria type Smoke Detector with Detector base for Utility area		
8	Intelligent Analogue Addressable Smoke Detector., UL Listed 268, software Programming only.		
9	Addressable Break Glass type Manual Call Point		
10	Addressable Monitor Modules		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
11	Addressable Control Modules		
12	100 DB Sounder		
13	Integration with PAC and BMS System		
14	All cables must be FRLS type. All conduits must be metal type.		
<b>OEM Qualification Criteria</b>			
1	Service Centre in Bhubaneswar		
2	At least 100 installations In India. Self-declaration from OEM to be submitted		
3	Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Fire Alarm System	1.5	Service Centre in Bhubaneswar	Yes	0.5
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.5
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

#### 5.22.18 Gas Based Fire Suppression System: - Suppression system (NOVEC 1230)

##### **Sizing: As per Bidders solution**

##### **Product/Solution Description**

Gas based fire suppression system is required to be used for Server room, UPS and Electrical rooms (for Data Centre floor). Cylinders for Server Hall is suggested to be placed on the outside the server hall on the exit path (near Staircase). There are three voids in the server hall. One is room void, second is floor void and third is containment void. All the voids have to be covered. There are 5 containments which have to be considered for gas and nozzle calculation.

##### **Scope of Work**

Removal of existing fire hydrant pipes and nozzles from the server farm area and handing over to estate department.  
 Supply of NOVEC 1230 cylinder with Gas, all accessories, installation, testing and commissioning of the same.  
 Maintenance for 5 years.

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	The bidder shall supply, install, test and put in operation (NOVEC) 1230 based fire suppression system. The fire suppression system shall include and not be limited to gas release control panel, CCOE approved seamless cylinders, discharge valve (with solenoid or pneumatic actuator), discharge pipe, non-return valve and all other accessories required to provide a complete operation system meeting applicable requirements of NFPA 2001 standards and installed in compliance with all applicable requirements of the local codes and standards.		
2	The work under this system shall consist of design, supply, installation, testing, training & handing over of all materials, equipment, hardware, software appliances and necessary labour to commission the said system, complete with all the required components strictly as per the enclosed tender specifications, design details. The scope also include the supply, installation & commissioning of any material or equipment including civil works that are not specifically mentioned in the specifications and design details but are required for successful commissioning of the project.		
3	The system design should be based on the specifications contained herein, NFPA 2001 & in accordance with the requirements specified in the design manual of the agent. The bidder, shall confirm compliance to the above along with their bid.		
4	The system shall be properly filled and supplied by an approved OEM (Original Equipment Manufacturer)		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
5	Generally the key components* of the system shall be VdS or LPCB or FM/UL listed. The NOVEC 1230 gas shall:		
6	Comply with NFPA 2001 or ISO 14520 standard and have the approval from US EPA (Environmental Protection Agency) for use as a total flooding fire extinguishing for the protection of occupied space:		
7	Must have zero ozone depletion potential (ODP)		
8	Have a short life span in the atmosphere, with atmospheric life time of less than 5 days		
9	Be efficient, effective and does not require excessive space and high pressure for storage;		
10	The system shall be designed taking the minimum design concentration as per NFPA 2001(Latest Edition) guidelines & as applicable to class 'A' & C risks. The NOVEC 1230 agent shall be stored in seamless steel cylinders and dry nitrogen shall be added to provide additional energy to give the required rapid discharge. At the normal operating pressure of 42bar at 21Deg C, the agent is a liquid in the container.		
11	As per the regulations of the Chief Controller of Explosives (CCE) Nagpur, any system which has a working pressure above 19 bar (280 psi) will require the use of seamless cylinders that have been duly approved by the CCE, Nagpur.		
12	ROOM INTEGRITY TEST		
13	NFPA2001 states that the design concentration of a clean agent post discharge shall be maintained for a sufficient period of time to ensure there is no re-ignition of fire once suppressed. NFPA 2001 and 12A require an enclosure integrity test as part of the acceptance procedure for all clean agent systems. This includes halocarbon and inert agents. This comprehensive test and calculation predicts the leakage area corresponding to the retention time of agent in the enclosure on discharge. Most specification state it must be ten minutes.		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	The cylinders must have digital pressure gauge which must be Capable of integration with DCIM tool for remote monitoring.		
14	Portable ABC /Co2 /Foam type Extinguisher for UPS, electrical room.		
<b>OEM Qualification Criteria</b>			
1	Service centre in Bhubaneswar		
2	At least 50 installations In India. Self-declaration from OEM to be submitted		
3	Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Gas Based Suppression System	1.5	Service Centre in Bhubaneswar	Yes	0.5
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.5
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

## 5.22.19 Access Control System

**Sizing: All doors to be controlled by card reader. Server hall entry by Biometric reader**

**Product/Solution Description**

**Access control system to the Data Centre will be at 3 level. Starting from the entry to the facility to the Server hall, support area, UPS and electrical room, all entry and exits to be controlled.**

**Scope of Work**

**Supply, Installation, Testing and commissioning of Access control system with all accessories**

**Maintenance for 5 years**

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	The Integrated Access Control System's (ACS) primary function shall be to regulate access through specific doors, gates or barriers to secured areas of the facility.		
2	An Intelligent System Controller (ISC) shall link the ACS software to all other field hardware. It shall provide full distributed processing for access control and alarm monitoring operations. Controller should be 8 doors, 40,000 cards capacity, and 10000 events. Interface on RS232, RS485 and TCP/IP.		
3	A Dual Reader Interface Module (DRIM) shall be available for each controlled door and provide the ability to connect up to two card readers or entry devices		
4	Smart card readers at every Critical door for Entry and Exist. Biometric finger print Card reader for Critical door of Server room Door only for Entry Point and exist Smart card readers.		
5	Enterprise Version Server Software for Access control & Time and Attendance with capability to service Minimum 1 concurrent clients, Inclusive of One Server & One Client License.		
6	Shall be capable to communicate with centralized command software (BMS).		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
7	Software shall Programmable functions, controller downloads and uploads, multi-level local and global anti-pass-back, integration with fire systems, grouping of escape routes, door security clearance, import and export utilities, etc.		
8	• Multiple layers of maps with interactive icons;		
9	• Alarm recognition and treatment;		
10	• Scheduled times for door clearance;		
11	• Send emails and SMS to selected users; • Multiple card formats and facility codes;		
12	• Flexible commands for card users such as temporary access level (shift changes) and provisional cards, card lock, penalties, card and event tracking, Double custody of access cards, etc.; • control, multi-level locker and rack control with required Hardware controller		
13	SITC of Multi Format Card Readers		
14	SITC of Biometric + Smart Card Readers, shall have 2" IPS (In Plane Switching) touch screen LCD with Corning Glass scratchproof protective glass with Smart card reader module. Authentication shall be done in 1 second and the 1GB memory on board for user storage of minimum 5000 users with a card & 25000 events transaction log capability.		
15	SITC for Panic Bar with alarm for emergency exit doors.		
<b>OEM Qualification Criteria</b>			
1	Service centre in Bhubaneswar		
2	At least 100 installations In India. Self-declaration from OEM to be submitted		
3	Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.		



**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	Access Control System	1	Service Centre in Bhubaneswar	Yes	0.34
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.33
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.33
				No	0

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

## 5.22.20 High Sensitivity Smoke Detection System

**Sizing: As per bidders solution****Product/Solution Description**

A high performance aspirating smoke detection system shall be supplied, installed and commissioned by the specialist contractor in accordance with the requirements detailed in the NFPA – 72, Aspirating Detection Systems.

**Scope of Work**

**Supply, Installation, Testing and commissioning of Access control system with all accessories  
Maintenance for 5 years**

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/ Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	The panels shall be mounted inside the risk protected and there shall be a network of air sampling pipe work.		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
2	The High Sensitivity Smoke detection consist of highly sensitive Laser-based Smoke Detectors with aspirators connected to networks of sampling pipes. The alarms are generated once the laser sensor receives smoke at a pre-determined obscuration level to activate and alert, Fire 1, Fire 2 and alert signal.		
3	The signal is extended to the Fire Alarm monitor Modules / BMS through Volt free contacts for further investigation.		
4	When required, it shall be possible to connect an interface card for open Protocol output to BMS system for online Monitoring with Software level integration.		
5	When required, an optional remote Display unit shall be provided to monitor each detector, and a Programmer shall be supplied to configure the system.		
6	The system shall include all equipment's, appliances and labor necessary to install the system, complete with high sensitive LASER-based 7Smoke Detectors with aspirators connected to network of sampling pipes.		
7	The Bidder shall also make provision in the Aspirating Smoke Detectors to trip PAC system and to shut fire dampers in the event of fire through the relay contacts.		
8	Codes and standards The entire installation shall be installed to comply one or more of the following codes and standards :  NFPA Standards, British Standards, BS 5839 part :1		
9	Approvals  All the equipment's shall be tested, approved, and/or listed by : o LPCB (Loss Prevention Certification Board), UK FM Approved for hazardous locations Class 1,Div 2 UL (Underwriters Laboratories Inc.), US ULC (Underwriters Laboratories Canada), Canada o Vds (Verband der Sachversicherer e.V), Germany		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
10	The System shall consist of a high sensitive LASER-based smoke detector, aspirator, and filter.		
11	It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a programmer that is either integral to the system, portable or PC based.		
12	<p>The system shall allow programming of: Multiple Smoke Threshold Alarm Levels Time Delays.</p> <p>Faults including airflow, detector, power, filter block and network as well as an indication of the urgency of the fault. Configurable relay outputs for remote indication of alarm and fault Conditions. It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modelling tool. Optional equipment may include intelligent remote displays and/or a high level interface with the building fire alarm system, or a dedicated System Management graphics package.</p>		
13	<p>Performance Requirements Shall provide very early smoke detection and provide multiple output levels corresponding to Alert, Action, and Fire 1 &amp; 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter Shall report any fault on the unit by using configurable fault output relays or via the graphics Software. Shall monitor for filter contamination. Shall incorporate a flow sensor in each pipe and provide staged airflow faults.</p>		
14	<p>Materials and Equipment's Both Light Scattering and Particle Counting shall be utilized in the device as follows: The Laser detection Chamber shall be of the mass Light Scattering type and capable of detecting a wide range of smoke particle types of varying size. A particle counting method shall be employed for the purposes of Preventing large particles from affecting the true smoke reading.</p>		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	<p>Monitoring contamination of the filter (dust &amp; dirt etc.) to notify automatically when maintenance is required.</p> <p>The Laser Detection Chamber shall incorporate a separate secondary clean air feed from the filter; providing clean air barriers across critical detector optics to eliminate internal detector contamination.</p> <p>The detector shall not use adaptive algorithms to adjust the sensitivity from the set during commissioning. A learning tool shall be provided to ensure the best selection of appropriate alarm thresholds during the commissioning process.</p>		
15	<p><b>Detector Assembly</b></p> <p>The Detector, Filter, Aspirator and Relay Outputs shall be housed in a mounting box and shall be arranged in such a way that air is drawn continuously from the fire risk area by the Aspirator and a sample passed through the Dual Stage Filter and then to the detector.</p> <p>The detector shall be LASER-based and shall have an obscuration sensitivity range of 0.025 – 20% obs/m.</p> <p>The detector shall have four programmable smoke alarm thresholds across its sensitivity range with adjustable time delays for each threshold between 0 - 60 seconds.</p> <p>The detector shall also incorporate the facility to transmit a fault through a relay.</p> <p>The detector shall have a single pipe inlet that must contain an ultrasonic flow sensor. High flow fault (urgent and non-urgent) and low flow fault (urgent and non-urgent) can be reported.</p> <p>The filter must be a two-stage disposable filter cartridge. The first stage shall be capable of filtering particles in excess of 20 microns from the air sample. The second stage shall be ultra-fine, removing more than 99% of contaminant particles of 0.3 microns or larger, to provide a clean air barrier around the detector’s optics to prevent contamination and increase service life.</p> <p>The aspirator shall be a purpose-designed rotary vane air pump. It shall be capable of allowing/ supporting for a single pipe run /</p>		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	<p>multiple sampling pipe runs with a transport time of less than 90 seconds.</p> <p>Detectors shall be capable of supporting a single pipe run of 25m with a maximum transport time of 120 seconds or as appropriate standards dictate.</p> <p>The Assembly must contain relays for fire 1, Action and fault conditions. The relays shall be software programmable (latching or non-latching). The relays must be rated at 2 A at 30V DC. Remote relays shall be offered as an option and either configured to replicate those on the detector or programmed differently.</p> <p>The Assembly shall have built-in event and smoke logging. It shall store smoke levels, alarm conditions, operator actions and faults. The date and time of each event shall be recorded. Each detector (Zone) shall be capable of storing up to 18000 events.</p>		
16	<p>Displays on the Detector Assembly</p> <p>The detector will be provided with LED indicators.</p> <p>Each Detector shall provide the following features at a minimum.</p> <p>Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector. o Smoke Dial display represents the level of smoke present.</p> <p>Fault Indicator.</p> <p>Disabled indicator.</p> <p>Buttons supporting the following features shall be accessible to authorized personnel.</p> <p>Reset – Unlatches all latched alarm and faults.</p> <p>Disable – Disables the fire relay outputs from actuating and indicates a fault.</p>		
17	<p>Sampling Pipe</p> <p>The sampling pipe shall be smooth bore with an outside diameter of 25mm and internal diameter of 21mm should be used.</p> <p>The pipe material should be suitable for the environment in which it is installed, or should be the material as required by the specifying body.</p> <p>All joints in the sampling pipe must be air tight and made by using solvent cement, except at entry to the detector</p>		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	<p>The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards.</p> <p>All pipes should be supported at not less than 1.5m centres, or that of the local codes or standards.</p> <p>The far end of each trunk or branch pipe shall be fitted an end cap and drilled with a hole appropriately sized to achieve the performance as specified and as calculated by the system design.</p>		
18	<p><b>Sampling Holes</b> Sampling Holes of 2mm, or otherwise appropriately sized holes, shall not be separated by more than the maximum distance allowable for conventional detectors as specified in the local codes &amp; standards. Intervals may vary according to calculations.</p> <p>Each sampling point shall be identified in accordance with Codes or Standards. Consideration shall be given to the manufacturer's recommendations and standards in relation to the number of Sampling Points and the distance of the Sampling Points from the ceiling and roof structure and forced ventilation systems.</p>		
<b>OEM Qualification Criteria</b>			
1	Service centre in Bhubaneswar		
2	At least 100 installations In India. Self-declaration from OEM to be submitted		
3	Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.		

**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	HSSD	1.5	Service Centre in Bhubaneswar	Yes	0.5
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.5
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.5
				No	0

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

5.22.22 IP Based CCTV System

**Sizing: All area inside and outside the Data Centre to be covered under surveillance.**

<p><b>Product/Solution Description</b></p> <p><b>All areas to be covered under surveillance. Inside the server hall all aisles to be covered. No dark spot inside the server hall and support area except manager’s cabins.</b></p> <p><b>Scope of Work</b></p> <p><b>Supply, installation, testing and commissioning of IP CCTV system Maintenance for 5 years.</b></p>
--

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	2 megapixel (1920 x 1080) resolution Indoor Camera with 1/2.9" 2.19M CMOS or better , Lens- 3.2 ~ 10mm varifocal lens or better ,Min 30fps@all resolutions (H.264), H.264, MJPEG codec supported, Multiple streaming and User Access 6 users at unicast , Auto Day & Night ,WDR -120dB or better, Tampering, Motion detection, Micro SD/SDHC memory slot Min support 32GB, PoE , Hallway view, IR Range 20m		

2	2 megapixel (1920 x 1080) resolution weather proof bullet type camera with /2.9" 2.19M CMOS, Lens 3.2 ~ 10mm varifocal lens or better, Min 30fps@all resolutions (H.264), H.264, MJPEG codec supported, Multiple streaming and User Access 6 users at unicast , Auto Day & Night ,WDR -120dB or better, Tampering, Motion detection, Micro SD/SDHC memory slot Min support 32GB, PoE , Hallway view, IR Range 30m, IP66 support		
3	2MP (1920 x 1080) resolution outdoor PTZ camera with 1/2.8" 2M CMOS , Focal Length 5 ~ 100mm , zoom 20X , Pan-360° Endless, Tilt Range200° ,Pan / Tilt Speed-P reset : 500°/sec, Manual : 0.24°/sec ~ 200°/sec, Pre-set -300, Swing, Group , Trace, Tour (1ea), Auto run, ScheduleH.265, H.264, MJPEG codec support, Multiple streaming, auto Day & Night (ICR), HLC/ BLC WDR120 dB, DIS with Built-in Gyro sensor, Tampering, Motion detection, Memory slot and support Min 256GB, IP66, IK10		
4	32CH, Max. 12MP Camera supported, 256Mbps network camera recording, Transmission Bandwidth 500Mbps, Support 4K video out on HDMI monitor, Simultaneous Playback Min 16CH Support Dual monitor video out, Support H.265, H.264, MJPEG compression, . 8 internal HDDs support e-SATA / iSCSI external storage, backup from camera SD card & Failover support- N+N / N+1, Operating Temperature +0°C ~ +40°C, Humidity 20% ~ 85% RH or better.		
5	There should be provision of integration of CCTV system with DCIM tool in order to monitor the Camera, NVR, HDD status remotely.		
<b>OEM Qualification Criteria</b>			
1	Service centre in Bhubaneswar		
2	At least 100 installations In India. Self-declaration from OEM to be submitted		
3	Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.		



**Evaluation Criteria:**

Sl.	Name of the Device	Max. Score	Parameter	Specification	Score
#	CCTV	1	Service Centre in Bhubaneswar	Yes	0.34
				No	0
			At least 100 installations In India. Self-declaration from OEM to be submitted	Yes	0.33
				No	0
			Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.	Yes	0.33
				No	0

**N.B: Supporting Document to be submitted for the above specification:** Product Catalogue from OEM with clearly highlighted portions of the mentioned parameters or undertaking in the letter head of the OEM for availability of the desired parameter/feature.

**5.22.23 Water Leakage Detection System****Rating/Sizing: 4 / 8 zones****Product/Solution Description**

A central control apparatus electrically interconnected with a plurality of circuits which enable water leaks to be accurately detected in a diversity of devices including air conditioners, compressor coils, hot water appliances, and pipes, and for communicating the severity of the water-related problem. A plurality of water sensors are incorporated into specially designed probes of the preferred embodiment wherein water leaks may be accurately and reliably detected in a diversity of water-dependent appliances and devices. The product shall be designed and should be easily installed and to be inherently devoid of any safety hazards. The total area under protection shall be divided into multiple zones. When there is a potential leak detected, the product shall be able to locate the zone(s) in which the leak has occurred with the corresponding zone name.

**Scope of Work**

Supply, Installation, testing and commissioning of Water leak detection system  
Maintenance for 5 years

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	Control Panel with 4 x 20 LCD		
2	4 / 8 zones		
3	Sensing technology shall be only AC		

4	Isolate facility for each zone		
5	Common fire interface relay		
6	Fault relay		
7	Hooter output		
8	Zone alarm & fault LED Indication		
9	MODBUS RTU for BMS integration		
10	The complete system shall include an electronic System control panel, multiple control modules , distance type sensing cable and all required auxiliary accessories (such as hold down clip & Tag/Label for the sensing cable).		
11	This system shall detect and locate multiple leaks simultaneously as well as cable break & power failure and activate the control panel alarm relays. The sensing cables shall be of such construction that no metallic parts shall be exposed to the environment. The system shall be provided with the flexibility of custom "cut-to-length" sensing cable to meet the exact length requirement at each area of protection and with pre-connectors sensing cable components.		
<b>OEM Qualification Criteria</b>			
1	Service centre in Bhubaneswar		
2	At least 100 installations In India. Self-declaration from OEM to be submitted		
3	Must have installation in at least 5 Data Centres in India. Documentary proof to be submitted.		

#### 5.22.24 Ultrasonic Rodent Repellent system

##### Rating/Sizing:

##### Product/Solution Description

The objective is to protect the entire premise all the voids against rodents. The purpose is to keep the rodents away from the floor by generating very high frequency sound waves (above 20 Khz) which are not legible to human ear but irritates rodents. The objective is to protect all the cables below floor, above ceiling & room void from damage caused by rodents.

##### Scope of Work

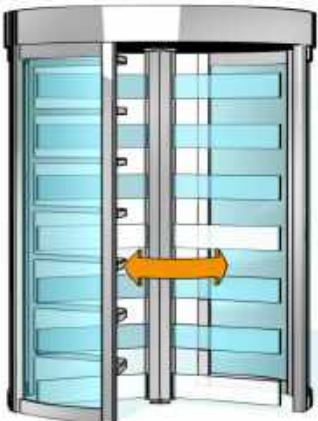
Supply, Installation, testing and commissioning of Water leak detection system  
 Maintenance for 5 years  
 Rodent Repellent system shall be provided on in all voids.

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	2x16 LCD		
2	System Healthy relay		
3	Mini Exhaust Fan		
4	RS485 MODBUS RTU for BMS Integration		
5	Test Transducer Menu		
6	Programmable Sweep Time & delay		

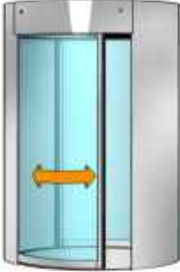
5.22.25 Physical Access Control System


**Rating/Sizing: Full height**

<b>Product/Solution Description</b>
<b>Scope of Work</b>

S.No	Requirement	Compliance (Fully or better complied/ Partially complied/ Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
A	<b>Full Height Turnstile for Data Centre Entrance</b>		
	<p><b>Standard measurements:</b></p> <div data-bbox="343 1077 662 1496" style="text-align: center;">  </div> <p data-bbox="416 1525 560 1556">Fig. No-17</p> <p><b>Construction:</b></p>		

S.No	Requirement	Compliance (Fully or better complied/ Partially complied/ Not complied)	Remark (If any)
	<p>The side body parts are designed with LSG 8 mm glass panels and connected with one another in the area of the centre post. The upper dustproof cover is made from raw aluminum plating. Two maintenance openings are integrated into the lower ceiling plate; the outer maintenance opening can be locked, designed for Euro profile half cylinders of the customer. 120° rotating unit: tubular column, Ø 89 mm, each with 7 U-shaped crossbars, made of glossy stainless steel AISI 304. The blocking element on the side wall is made of rectangular aluminium profiles.</p> <p><b>Finish:</b> Plastic coated in an RAL colour or anodized natural tone.</p> <p><b>Function:</b> The security revolving door is equipped with a 1.6 joule limited low energy SK-M servo positioning drive for automatic access control and active locking. The selected rotation direction is released for a rotary cycle by a floating signal initiated by an on-site element (or one supplied by the customer). The selected rotation direction is released by a release impulse for the entry or exit direction. The rotary motion is started by manually pushing the turnstile. The rotating unit is then automatically turned by a motor to the next home position and locks. If no one passes through the security revolving door within an adjustable period of time, the release is cancelled. The behaviour of the end point locking in the event of a power failure can be freely selected. Standard setting: blocked in entry direction, free rotation in exit direction. It is not possible for people to get jammed or stuck thanks to the patented end point locking.</p> <p><b>Electrical system:</b> The network-compatible CAN bus control unit is integrated into the unit. Power supply 100–240 VAC 50/60 Hz 253 VA. Four floating inputs for on-site control and five floating outputs for further on-site processing.</p>		
	<b>Personal Interlock System for DC Entrance</b>		
	<b>Standard measurements:</b>		

S.No	Requirement	Compliance (Fully or better complied/ Partially complied/ Not complied)	Remark (If any)
	<p>Total height: 2400 mm                      Headroom: 2100 mm                      Outside diameter: 1020, 1220 mm                      Passage width: 550, 680 mm                      Upper part of the body: 300 mm</p> <p><b>Construction:</b>                      The interlock has a steel structure with metal cladding. The control unit and drive are integrated into the upper part of the body. The upper dustproof cover is made from raw aluminium plating. There is a maintenance opening in the lower ceiling plate. Two closable maintenance openings are integrated into the covers above the door leaves.</p>  <p style="text-align: center;">Fig. No-18</p> <p>The sliding wings are made of aluminium profiles with LSG 10 mm glazing flush-sealed to the outside. Moving safety strips for personal security are installed in the door leaves. There is a light scanner and a contact mat in the interlock with a zone for presence detection. Inner sidewalls limit the interlock space to the passage width of the interlock. A safety strip on the inner side wall protects fingers from getting stuck in the door leaf. Two LED lights, approx. 30,000 h service life, are integrated into the ceiling plate. Including floor element with guidance system and mounting of the security contact mat with black rubber nub covering.</p> <p><b>Finish:</b>                      Powder-coated in an RAL colour or anodised natural tone C0</p> <p><b>Function:</b>                      The first sliding door is opened by a motor-driven system in the direction of entry or exit by a floating release signal by the customer. The door closes and locks automatically after the inner area of the interlock has been entered. Then the second sliding door opens. After the person leaves the personal interlock, it closes and locks. If no one enters the interlock within an adjustable time period after release, the release is cancelled. There is an emergency release switch in the interlock that opens the outer door when pressed. The interlock control unit prevents both sliding doors from opening at the same time. The behaviour of the sliding</p>		

S.No	Requirement	Compliance (Fully or better complied/ Partially complied/ Not complied)	Remark (If any)
	<p>doors in the event of a power failure can be freely selected. Standard adjustment is inside closed and locked, outside open.</p> <p><b>Electrical system:</b></p> <p>The network-compatible CAN bus control unit is integrated into the unit. Power supply 230V AC 50/60 Hz.</p> <p>Four floating inputs for on-site control and five floating outputs for further on-site processing by the customer are available.</p>		
B	<p><b><u>Supply of Sensor Swing Barrier:-</u></b></p>  <p>Fig. No-19</p> <p>(1) Two wings/door leaves are made of transparent polycarbonate with 10 mm thickness, upper edge 900 mm with opening/ closing time of 0.3 seconds minimum, which can be adjusted as per client requirement. (2) Design: The housing and the base columns are made of AISI 304 stainless steel. Finish: Stainless steel semi-gloss smooth finish. (3) Function: The sensor barrier is equipped with two servo positioning drives (low energy drives with energy content &lt;1.6 joules) along with Tooth holding brake technology and is electrically controlled in both directions thus guaranteeing a particularly high level of personal safety. The passage area is monitored by a basic sensor system with a short design. It monitors the individual passages in both directions. This sensor system also monitors the swinging area and the blocking elements and acts as a protection device. In the event of a power failure, both directions may be freely accessed. Automatic reset upon resumption of power supply – the unit resets to its regular function without manual intervention. The access area is secured immediately upon resumption of power supply. The unit can be locked in any position (Tooth Holding Brake Technology) and opens under load (personal safety in case of panic). In basic position, the unit is unlocked to minimize power consumption. Parameters can be set for unit behaviour and each specific customer (e.g. starting behaviour and passage speed). (4) Standard measurements: Total width: 1,070 mm, passage width: 650 N/900 W mm, interlock height: 945 mm &amp;</p>		

S.No	Requirement	Compliance (Fully or better complied/ Partially complied/ Not complied)	Remark (If any)
	wings height 900 mm and total length 1660 mm (5) MCBF: Complete swing flap barrier unit/system MCBF (mean cycles between failures) is 8 million for 650 mm passage width and 6 million for 900 mm passage width (6) standby power consumption 17 VA (7) flap barrier should have a inbuilt counter to count the cycles entry and exit and if required a output should be given displaying the count on any display. 4 lane configurations with 3 normal lanes passage width 650 mm + 1 wider lane passage width 900 mm. =		
<b>Desired Technical Requirements</b>			
1	servo positioning drives		
2	standby power consumption 17 VA swing flap barrier		
3	Wings opening/ closing time should be 0.3 seconds minimum, which can be adjusted as per client requirement		
<b>OEM Qualification Criteria</b>			
1	Service support all major cities in India		
2	Origin of manufacturing. Note: China make product's will not be not accepted.		

#### 5.22.26 3D X-ray Baggage Scanner

**Rating/Sizing: As per bidder solution**

<p><b>Product/Solution Description</b> 3D X-ray Baggage Scanners</p> <p><b>Scope of Work</b> SUPPLY INSTALLATION TESTING COMMISSIONING OF X-RAY BAGGAGE SCANNERS</p>
--

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/ Not complied)	Remark (If any)
<b>Mandatory Technical Requirements</b>			
1	X Ray baggage Scanner Technology should be based on Dual energy based isometric X-Ray imaging.		
2	The Baggage scanner should produce isometric view (virtual 3D view) of the		



Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	objects scanned to have more detailed information, which are not visible in traditional single view baggage scanners, which generates only the top or bottom (2D) view of the scanned objects.		
3	Machine should generate the images in such a way that the depth of any scanned object can be visualized appropriately to further analyse the details of the object inside a baggage for better identification of harmful objects like Gun/Knife etc.		
4	Tunnel Size - Minimum 60 cm W (width) x Minimum 40 cm H (Height)		
5	Operating System : LINUX		
6	Equipment manufacturer should have ISO 9001 certified factory in India. Certificate to be submitted.		
7	Production license from AERB should be submitted.		
8	Preference for equipment manufactured by MSME registered OEM.		
9	Preference to OEMs as per Make In India Policy will be given.		
<b>Desired Technical Requirements</b>			
1	Conveyor belt speed should be between 0.2 and 0.3 meter per second. Conveyor movement bi-directional		
2	All machines should operate on 230 VAC, 50 Hz power supply		
3	Conveyor Capacity - 160 kg evenly distributed		
4	Through put should be 500 bags per hour		
5	Tube Voltage : Maximum 160 kVA		
6	Tube Current 0.3 to 1.2 mA (Must be Adjustable); Duty Cycle - 100%		
7	The X-ray beam divergence should be such that the complete image at maximum size of bag is displayed without corner cuts.		
8	The radiation level should not exceed accepted health standard (0.1m R/Hr at a		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	distance of 5 CM from external housing). Relevant certificate from AERB		
9	<ol style="list-style-type: none"> <li>The operating temperature should be - 5° to 50° C (Test Certificate from NABL accredited Lab to be submitted at the time of bidding)</li> <li>Storage temperature - 20° to 60° C (Test Certificate from NABL accredited Lab to be submitted at the time of bidding)</li> <li>Relative Humidity- 10 to 95% non-condensing</li> </ol>		
10	Resolution: The machine should be able to display single un-insulated tinned copper wire of 42-SWG or 38-AWG		
11	Steel penetration: 30 mm or above		
12	Sensors > 1000 diodes, L-shaped detector (folded array type)		
13	Video display - 17" or better LCD Monitor High resolution, low radiation, flicker free, resolution at least 1280x1024, 24 bit true color real time processing		
14	<b>Health &amp; Safety</b> - The machine must comply with requirements of health and safety regulations with regards to mechanical, Electrical and radiation hazards. The supplier/manufactures should furnish Test Certificate from Atomic Energy Regulatory Board of India regarding radiation safety.		
15	<b>Computer Specifications -</b> <ol style="list-style-type: none"> <li>Processor: Intel i3 or better</li> <li>Memory: 4GB RAM</li> <li>Storage: 160GB HDD</li> <li>Video Card: 512MB Graphic card</li> <li>Backup: UPS (10 Min) for Computer</li> </ol>		
16	<b>Other Features</b> <ol style="list-style-type: none"> <li>Multi energy imaging (4 color palette)</li> </ol>		

Sl. No	Requirement	Compliance (Fully or better complied/ Partially complied/Not complied)	Remark (If any)
	2. Crystal clear images 3. Black & white viewing 4. Organic/ inorganic stripping 5. High penetration 6. Variable edge enhancement 7. Zoom 32 X or more 8. Facility to view previous bag 9. Manual image archive 10. Configurable image processing keys 11. Facility to count baggage 12. Date /time display 13. Have search indicator 14. Have facility of high-density alert (HDA) 15. Manual Scan facility 16. Automatic image archiving		
17	<b>Film Safety:</b> Guaranteed safety for high-speed films up to ISO1600. The machines should be film safe. In other words, photographic films must not be damaged due to x-ray examination		
18	Threat image projection (TIP)		
19	Input/ Output Rollers - 0.5 mtr length each		

## 6. Detailed Scope of Work

The minimum specified scope of work to be undertaken by the bidder for Design, Supply, Installation, testing, Commissioning, Operations and Maintenance of the proposed OSDC 2.0 at Bhubaneswar as per the scope mentioned below. The selected bidder shall ensure an uptime more than 99.982% on a quarterly basis for period of five years after Go Live.

The minimum specified work to be undertaken by the bidder for setting up and operating the proposed Data Centre OSDC 2.0, has been categorized as under:

- d. Develop appropriate design, make all required approval, Supply building material, built a Civil (building) infrastructure including associated works of the proposed OSDC 2.0 at Bhubaneswar
- e. Supply, Installation, testing and commissioning of the Non-IT Infrastructure of the proposed OSDC 2.0 at Bhubaneswar
- f. Supply, Installation, testing and commissioning of the IT Infrastructure of the proposed OSDC 2.0 at Bhubaneswar
- g. Data & Application migration from currently working State Data Centre to new Data Centre OSDC 2.0.
- h. Operations and Maintenance services for the complete Infrastructure at OSDC 2.0 at Bhubaneswar for the period of 5 years from the date of successful acceptance by OCAC.

*Note: The bidders are requested to submit their proposals for these Schedules in the same bid which would be combined for evaluation purposes.*

### 6.1. Tier Certification by Uptime Institute

The bidder has to ensure that the Data centre gets certified for Tier III or higher as feasible and suitable from Uptime Institute Inc.

The Data Centre Facility to be constructed under this contract shall be Uptime Institute Tier III/Tier IV Gold Certified. The successful bidder shall obtain the following as part of this certification process:

- Tier III/IV Certification of Design Documents for Complete Data Centre Facility Design
- Tier III/IV Certification of Constructed Facility for all areas of Data Centre Facility to be constructed under this contract
- Tier III/IV Certification of Operational Sustainability
- All Certifications shall be kept valid for the contract period
- The necessary certifications will be obtained on the behalf of the client and passed on to them on award.
- Bidder has to offer rates for all three certifications separately.

The successful bidder shall be responsible for all associated cost for obtaining & maintaining these certifications.

## 6.2. IT System Design Consideration

### 6.2.1 SITC of IT Infrastructure:

As a way forward, the broad scope of work under this phase will include the following, but is not limited to:

OSDC 2.0 is envisaged to establish a robust infrastructure to enable the Government of Odisha to deliver the services quickly and effectively to its stakeholders. State Government aims to create a highly secure flexible, automated, managed cloud service environment deploying the latest industry computing infrastructure for keeping the user department applications secure, highly scalable and available.

The objective is to provide logically unified and shared infrastructure flexible enough to rapidly respond to infrastructure requirements and also accommodate future technology enhancements, distributed applications, database applications running on bare metal, virtualized applications running in multi-hypervisor environments, and cloud-based applications that are available on demand all impose different demands on infrastructure.

Bidder will be expected to bring all the installation equipment's and tools required for the installation of the system. The Bidder shall install, integrate and commission the active network equipment as well as passive network components as per approved deployment design. All the work shall be done in a conscientious manner as per the OEM guidelines and best industry practices. The system shall be subjected to inspection at various stages. Local regulation / codes shall be followed at all times. The Bidder shall follow all Safety Regulations and practices. The Bidder shall not cause any damage to the existing server farm of OSDC, Government buildings /other premises and property and will perform restoration if any damage occurs. Trenches, path-cutting, etc. will be back-filled and restored to the original condition immediately after laying of the conduit/cable. The Bidder shall plug conduits and entrance holes where the cabling has been installed with suitable sealing material.

The Bidder has to establish centralized cloud environment that will be used to host multiple applications with simplified operations and increased application responsiveness to support a new generation of distributed applications while accommodating existing virtualized and non-virtualized environments.

- a. Deliver IT as a service starting with **IaaS, PaaS, CaaS, SaaS, DaaS**, etc.
- b. Deliver responsive IT based services to government/departments on demand at scale and anywhere.
- c. Deliver reliable User Experience

The IT infrastructure for OSDC 2.0 at Bhubaneswar will require various set of IT components for running their applications. Telecom racks would also be provided by Bidder. The Bidder is responsible to Supply, Install, Configure, Test and Maintain the entire solution for a period of five years from go live. The Bidder should propose only one solution that is in accordance with the RFP specifications.

The following is a list of categories of components that the Bidder is expected to supply, install, configure and test:

- a. Computing Infrastructure such as Servers, Operating Systems and Hypervisor etc.
- b. Network Infrastructure such as Routers, Spine and Leaf switches, SDN Controller etc.
- c. Security infrastructure such as Firewalls, HIPS, D-DOS, AAA, Anti-APT, DLP etc.

- d. Centralized Enterprise Management Solution, Patch Management, Antivirus, Cloud Management – Orchestration layer.
- e. Enterprise Class Storage Area Network along with Enterprise Class Storage system, SAN switches, Tape Library, etc.
- f. Operation and maintenance Services for a period of 5 years from Go-Live.

The above list is indicative, though the Bidder will be required to provide an infrastructure which is scalable and provides for next generation latest technologies like virtualisation, cloud computing, Orchestration etc. The Bidder is free to add any additional components that are deemed necessary for providing the overall solution as a whole. The Bidder should also consider the following while proposing the solution.

- i. The Bidder should ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to the devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
- ii. OCAC will not be responsible if the Bidder has not provisioned for any components, sub-components, assemblies, sub-assemblies as part of bill of material in the bid response. The Bidder will have to provision to meet the solution requirements, the same at no additional cost and time implications to OCAC.
- iii. The Bidder should ensure there is a 24x7x365 comprehensive onsite support arrangement for a period of 5 years after Go-Live with all the OEM for respective IT components.
- iv. It is expected that Bidder shall ensure that the equipment/components being supplied will be supported by respective OEMs for minimum 7 years from date of bid submission. If the same is de-supported by the OEM for any reason whatsoever, the Bidder shall replace it with an equivalent or better substitute that is acceptable to OCAC without any additional cost to OCAC and without impacting the performance of the solution in any manner whatsoever. Any components, subcomponents, assemblies, sub-assemblies (i.e. server, storage, OS) required for installation of EMS, Orchestration, backup, patch management, antivirus or any other software/management software needed for IT infrastructure will be provided by Bidder without any additional cost.

### 6.3. Key considerations for designing the Odisha State Data Centre 2.0:

#### I. Scalability

- A scalable system is one that can handle increasing numbers of requests without adversely affecting the response time and throughput of the system.
- The Data Centre should support both vertical (the growth of computational power within one operating environment) and horizontal scalability (leveraging multiple systems to work together on a common problem in parallel).
- Modular design of the Data Centre is an excellent strategy to address growth without major disruptions.
- All components of the data Centre must support scalability to provide continuous growth to meet the requirements and future demand from various existing or new departments.
- A scalable Data Centre shall easily be expanded or upgraded on demand. Scalability is important because new computing component is constantly being deployed, either to replace legacy component or to support new mission.

## II. High Availability

- Designing for high availability assumes that systems will fail, and therefore the systems are configured to mask and recover from component or server failures with minimum application outage.
- All components of the data Centre must provide adequate redundancy to ensure high availability of the e-Governance applications and other Data Centre services.
- The Bidder shall make the provision for high availability for all the services of the data Centre.
- Application availability is the responsibility of the application owner and the Bidder cannot be held responsible for any problem related to application and its availability.

## III. Interoperability

- The entire system/ subsystem should be interoperable, in order to support information flow and integration.
- Operating systems and storage technologies from several vendors must interact well with each other. These systems should also support the open architecture solutions where information/ data can be ported to any system, whenever desired.

## IV. Manageability

- The SDC must be designed in an efficient way to ensure an ease in maintenance.
- It must facilitate ease of configuration, ongoing health monitoring, and failure detection that are vital to the goals of scalability, availability, and security.
- The SDC shall be designed to match the growth of the environment including Infrastructure, Government data & information etc.

## V. Cyber Security

- The Data Centre must provide an end-to-end security blanket to protect applications, services, data and the infrastructure from intentional, unintentional or malicious attacks or theft from external (through internet) and internal (through intranet and or physical) hackers/malicious intent.
- Such attacks and theft should be controlled and well supported using next generation cyber security appliances e.g. Firewalls, IPS, WAF, AAA systems and infrastructure protection mechanisms.
- Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. It should be noted that at different layers of security, the make/model of the similar appliances should be different.

## VI. Integration of OSDC with SWAN

- Another most important aspect which should be taken care while designing the SDC is about seamless integration with SWAN.
- Provisioning of connectivity between the SDC and SWAN shall be the responsibility of OCAC such as laying of OFC, Cabling, etc. However the SI should be responsible for integrating SWAN link from the existing Data Centre to newly built Data Centre.
- Planning of terminating SWAN link should at gateway level of the Data Centre.

VII. IPv6 Readiness

- All the hardware and software (including but not limited to all the routers, switches, firewall, servers, and operating systems) supplied under this tender shall be IPv6 ready from day one.
- The performance as specified in the specification of each component in the RFP is for IPv6. These components should also be ready to work on IPv4 whenever required.
- The entire infrastructure should be configured & operational in IPv6 & IPv4 from day one i.e. in Dual Stack mode. In future, for migrated infrastructure in new DC, IPv6 shall be implemented in dual stack mode.

VIII. Cloud Services Provisioning

- The proposed Cloud solution should be capable of providing Infrastructure-as-a-Service and Platform-as-a-Service to various line departments within the State (Private Cloud). The detailed specifications of the Cloud is included in the section on Specification and Compliance requirements.
- The selected bidder will be responsible to take a transition of existing cloud solution from the existing Cloud service provider and will provide O&M support on co-ordination with the Cloud service provider.
- The selected bidder will also be responsible for migrating the existing cloud setup to the new Data Centre and integration will be made with the new cloud solution in the Data Centre which is proposed to be there.
- SI will co-ordinate with the cloud service providers (current and new) for migration and integration of existing cloud services and also will be responsible to monitor and manage the new cloud services which will be implemented in new Data Centre.

6.4. Inter -Intra Rack Connectivity

- i. Server will connect to the Leaf switch within the Rack on 10G/25G/40G.
- ii. Leaf switches will be connect with required no. of server racks for virtual environment on Day -1 maintaining redundancy.
- iii. 10 servers per Rack with 16G connectivity (1+1) to access SAN switch, 1 pair of SAN switch for every 3 Racks for virtual environment which means each SAN switch will have connectivity from Server to Access SAN switch.
- iv. SAN switches in pair will be required for requisite no. of server racks for cloud environment on Day -1

6.5. Indicative Logical Schematic

- i. Following is an indicative schematic of the Data Centre design architecture showing the major IT components that are to be provisioned by the Bidder.
- ii. OSDC 2.0 shall have compute environment.
- iii. OSDC 2.0 IT infra under this RFP shall be provisioned for approx. 90 racks environment. Centralized network/security infra will be common for both environment i.e. core switch, Firewall, IPS.



- iv. Racks will be loaded with network, security, compute, storage, Hypervisor, virtualization, orchestration etc.
- v. Storage, compute, hypervisor and other components shall not be provisioned for virtual environment.

### 6.5.1 High Level Indicative Logical Diagram for OSDC 2.0

Existing Network Diagram:

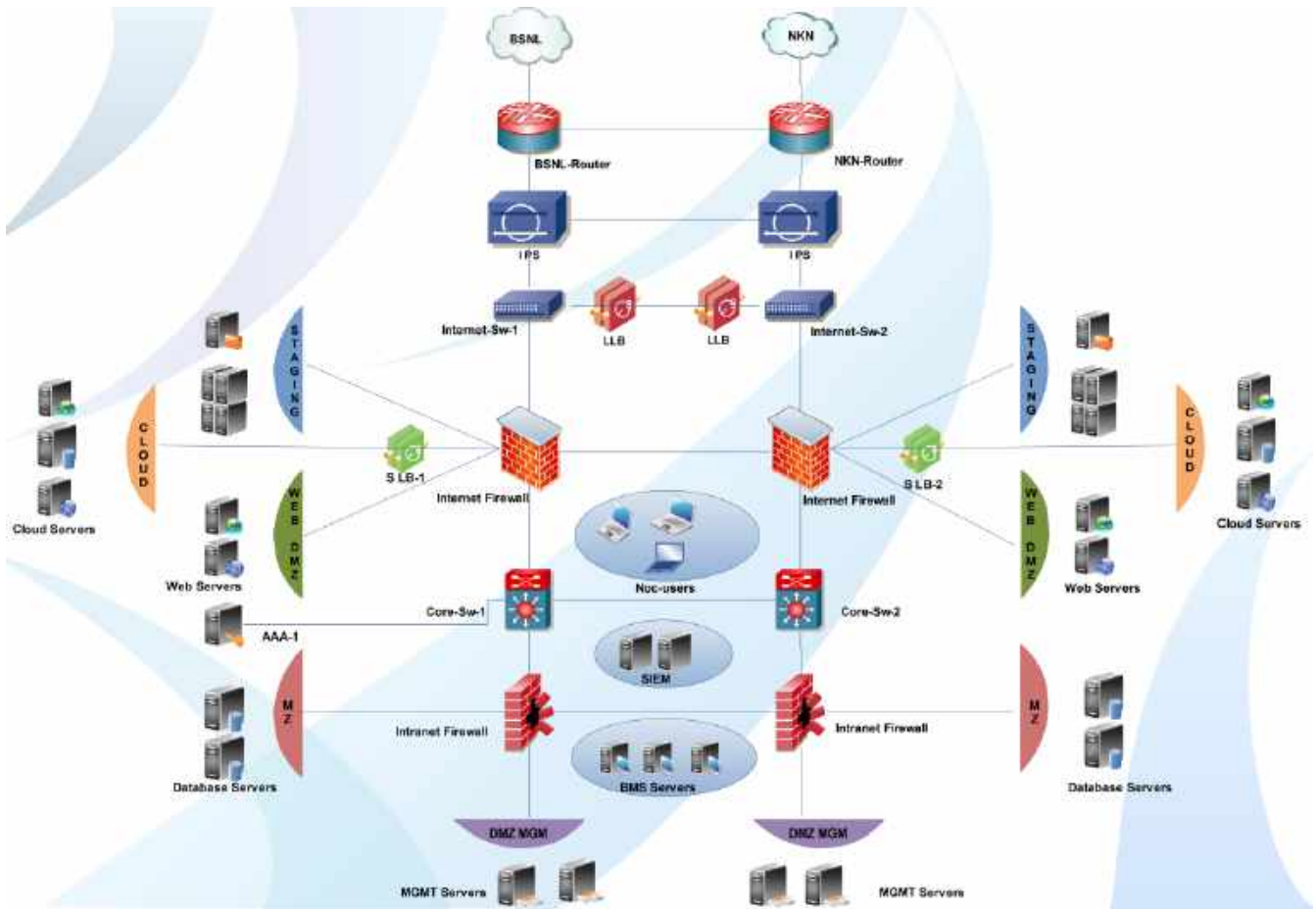


Fig. No-20

Proposed Indicative Network Diagram

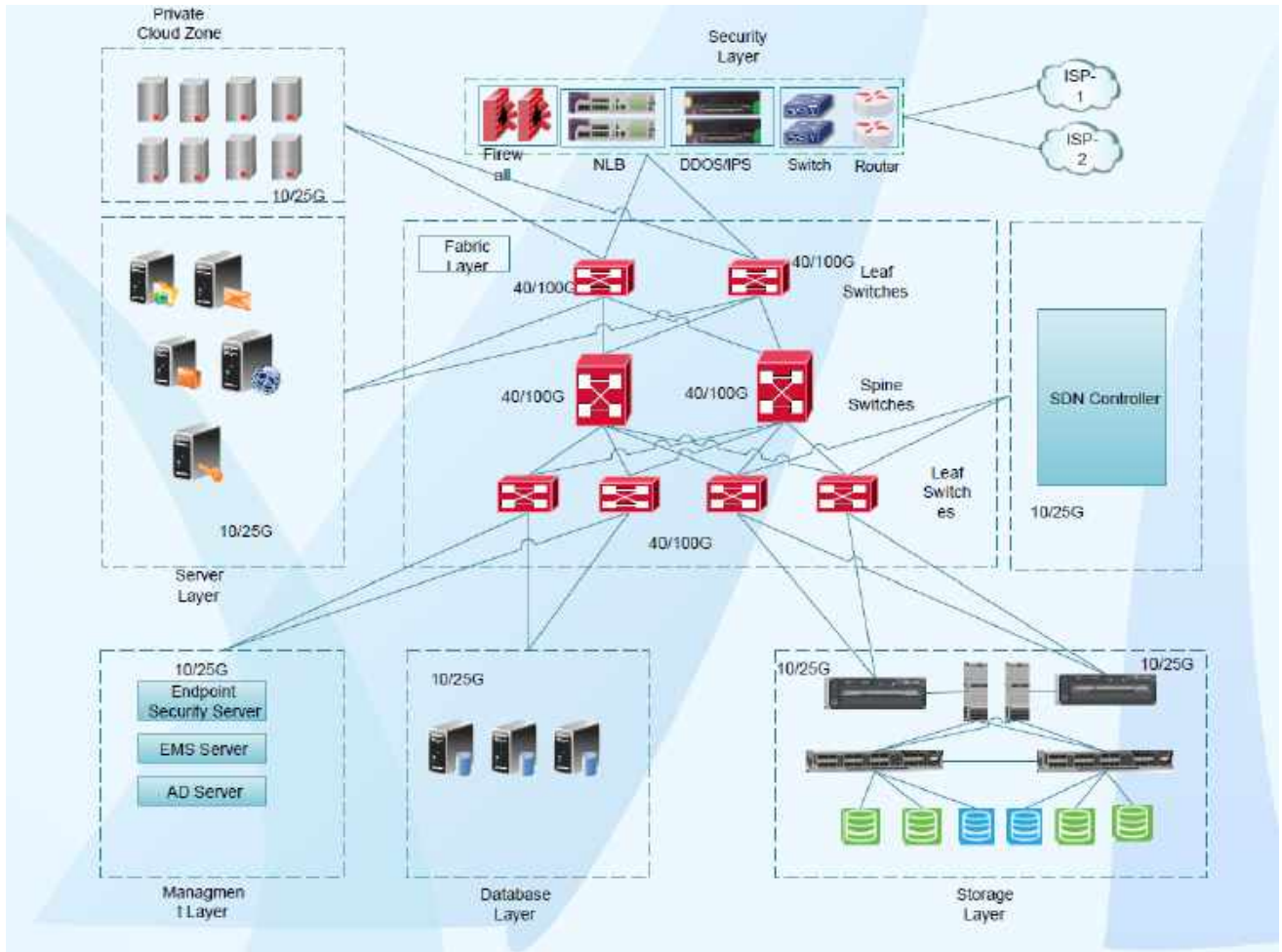


Fig. No-21

**ODISHA COMPUTER APPLICATIONS CENTRE**

**TENDER No. OCAC-NEGP-INFRA-008-2018-20038 Dated 09.10.2020**

**Name of Bidder**

< Name of Bidder >

**Summary of Total Bid for Odisha State Data Centre 2.0 Project**

#	Items Description	CAPEX Value	OPEX Value (As Annual Maintenance Cost)					Total Cost inclusive of all taxes (INR)
			Year 0 Cost	Year 1 Cost	Year 2 Cost	Year 3 Cost	Year 4 Cost	
1	Price Bid for SITC of Civil & Non IT Works							
2	Price Bid for SITC of IT Equipment (Hardware & Software)							
3	Price Bid for Uptime Institute Tier-III Design Certification Charges							
4	Price Bid for Half yearly health check Up							
5	Price bid for Liaison charges for Electrical Approvals form Electrical Inspector, Fire Department, PCB, PESO and other stationary bodies of Govt. of Odisha/India ( statutory charges if any will be payable by department.							
6	Price Bid for ISO 9001, ISO 27001 & ISO 20000 Certification Charges							
7	Price Bid for Integration & Migration							
8	Cost Bid for Manpower Cost for O&M for 5 years							

<b>9</b>	Price Bid for Operation & Maintenance for all Non-IT infrastructure for 5 Years							
<b>10</b>	Price Bid for Operation & Maintenance for all IT System for 5 Years							
<b>11</b>	Buyback price for existing hardware of SDC							
	<b>Total Cost</b>							
	<b>Grand total in Figure (Total Cost of Year 0 + Year 1+Year 2 +Year 3+Year 4 +Year 5)</b>							
	<b>Grand total in Word (Total Cost of Year 0 + Year 1+Year 2 +Year 3+Year 4 +Year 5)</b>							

Please Note.

1. 8x5xNBD Warranty certificate must be issue with the name of OCAC and shall submit to the OCAC.
2. All Optical/Electrical Transceivers should be from same OEM as the corresponding Switches/Router/Firewall etc..
3. Any other Hardware/Software required for the functional requirement of the project should be included in the total Bid price.
4. Bidder needs to evaluate their solution & requirements and in case of any additional requirement apart from the components mentioned above, it is bidders responsibility to consider the same.

**ODISHA COMPUTER APPLICATIONS CENTRE**

**TENDER No. OCAC-NEGP-INFRA-008-2018-20038 Dated 09.10.2020**

**Name of the Bidder:**

**Cost Bid for Civil and Non-IT Infrastructure**

#	Work Detail	UOM	Qty	Unit Rate for Year 0	Tax Rate & Amount for Year 0	Total Cost for Year 0
			A	U0	T0	TC0= (U0+T0)*Q
<b>A</b>	<b>CIVIL &amp; INTERIOR WORKS:</b>					
1	Dismantling existing Wall, Doors , Window or any structure of any material	Lot	1			
2	Removal of Debris from the site and disposing the same at a location as intimated by client	Lot	1			
3	Brick wall with plaster	Sqr Mtr	Bidder to Propose			
4	Closing of Doors, Windows if any with brick & plaster, Plywood, Gypsum etc.	Sqr Mtr	Bidder to Propose			
5	Creation of Ramp with desired top finish from outside to building ground floor	Cu Mtr	Bidder to Propose			
6	Creation of Toilet area with Male and female section including floor and wall tile fittings, plumbing, Electrical, doors, windows, exhausts etc. All fittings inside the toilet to be approved by OCAC before installation.	Lot	1			
7	Vitrified tile flooring	Sqr Mtr	Bidder to Propose			
8	Raise flooring in server hall of 300mm height	Sqr Mtr	350			
9	Skirting wherever required	Sqr Mtr	Bidder to Propose			
10	Gypsum partition 100 mm	Sqr Mtr	Bidder to Propose			
11	Glass partition - Fire rated	Sqr Mtr	Bidder to Propose			
12	Glass partition - Non fire rated	Sqr Mtr	Bidder to Propose			
13	Carpet flooring	Sqr Mtr	350			
14	PCC flooring	Sqr Mtr	900			
15	POP and Punning	Sqr Mtr	Bidder to Propose			
16	Epoxy flooring	Sqr Mtr	Bidder to Propose			
17	Anti-static PVC flooring	Sqr Mtr	Bidder to Propose			
18	Nitrile rubber Insulation 23 mm (minimum) under floor and roof including skirting	Sqr Mtr	850			
19	PCC flooring repairing	Sqr Mtr	Bidder to Propose			
20	Rolling shutter	Sqr Mtr	Bidder to Propose			
21	PVC door with frame	Nos	Bidder to Propose			

#	Work Detail	UOM	Qty	Unit Rate for Year 0	Tax Rate & Amount for Year 0	Total Cost for Year 0
			A	U0	T0	TC0= (U0+T0)*Q
22	Fire rated door - for UPS rooms- minimum width 1500mm - double leaf	Nos	2			
23	Fire rated door - Entry to server farm area from material lift lobby side. Minimum width 1500mm - double door	Nos	Bidder to Propose			
24	Fire rated door - Entry to staging room - single leaf - minimum width 1200 mm	Nos	Bidder to Propose			
25	Fire rated Glass door 1200 x 2300 single leaf	Nos	Bidder to Propose			
26	Designer privacy film on glass Door	Lot	1			
27	Flush door	Nos	Bidder to Propose			
28	Glass doors with all accessories	Nos	Bidder to Propose			
29	Modular false ceiling	Sqr Mtr	350			
30	Gypsum false ceiling	Sqr Mtr	100			
31	Fire rated paint	Sqr Mtr	Bidder to Propose			
32	Premium Emulsion paint	Sqr Mtr	Bidder to Propose			
33	Anti-Rust enamel Paint	Lot	1			
34	Exterior paint	Sqr Mtr	Bidder to Propose			
35	Earth pit cover	Nos	Bidder to Propose			
36	Earth Excavation	Cu Mtr	Bidder to Propose			
37	Earth refilling	Cu Mtr	Bidder to Propose			
38	Trench cover ( RCC)	Sqr Mtr	Bidder to Propose			
39	ISMB structure for ODU platform	KG	Bidder to Propose			
40	Security desk	Nos	2			
41	3+2 seater sofa along with tea table for waiting area near security	Nos	2			
42	Centre table for waiting area	Nos	2			
43	Reception table	Nos	1			
44	Modular workstation desk for office area	Seat	24			
45	Manager Table	Nos	3			
46	Meeting room table	Nos	2			
47	NOC technical desk	Nos	12			
48	Bunk bed (2Tier)	Nos	1			
49	Breakout area/Cafeteria Table	Nos	3			
50	Breakout area/Cafeteria Chair	Nos	9			
51	Staging room table	Nos	1			
52	Staging room chair	Nos	3			
53	NOC room Chair	Nos	12			
54	Workstation chair for office	Nos	24			
55	Conference table	Nos	1			
56	Conference chair	Nos	10			
57	Manager's chair	Nos	3			
58	Manager room visitor chair	Nos	9			

#	Work Detail	UOM	Qty	Unit Rate for Year 0	Tax Rate & Amount for Year 0	Total Cost for Year 0
			A	U0	T0	TC0= (U0+T0)*Q
59	Storage Units	Nos	Bidder to Propose			
60	Meeting room chair	Nos	6			
61	Other chairs	Nos	4			
62	Storage unit of 2 mtr height and 0.4 mtr depth, made of laminated particle board with shelves, lock and key.	Sqr Mtr	16			
63	Hand operated fork lift	Nos	1			
64	Paper shredder	Nos	1			
65	Water filter with RO facility	Nos	2			
66	Water dispenser	Nos	3			
67	Shoe stand 20 pair shoe capacity	Nos	2			
68	Steel Media storage 340 ltr	Nos	1			
69	Creation of steps with MDF board and top surface with vinyl and anti skiding tape	Sqr Mtr	Bidder to Propose			
70	DG foundation as per OEM specification	Cu Mtr	Bidder to Propose			
71	DG shed	Lot	Bidder to Propose			
72	Window vertical blinds	Sqr Mtr	Bidder to Propose			
73	Wire Mesh partition	Sqr Mtr	Bidder to Propose			
74	Fixed Iron Grill partition	Kg	Bidder to Propose			
75	Key Box	Nos	1			
76	Shoe Shiner ( dual shade electrically motor operated with sensor)	Nos	2			
77	Dust bin (Stainless steel)	Nos	15			
78	Tile puller (3 cup suction type)	Nos	3			
79	Vacuum Cleaner Industrial type	Nos	2			
80	Cold lock panels	Nos	Bidder to Propose			
81	Emergency Exit Ramp	Mtr	Bidder to Propose			
82	While board	Sqr Mtr	2			
83	Pin up Notice board	Sqr Mtr	2			
84	Refrigerator 300 Ltr	Nos	1			
85	Tea/ Coffee Vending machine	Nos	1			
<b>B</b>	<b>ELECTRICAL SYSTEM</b>					
87	HT Panel with 2 incomer and 2 outgoing and accessories	Nos	1			
88	Metering panel	Nos	2			
89	Dry type Transformer	Nos	2			
90	Removal of existing metring panel, HT cable, HT panel, Transformer, BBT, Transformer output panel etc.	Lot	1			
91	Transformer Output panel	Nos	2			
92	indoor/Outdoor/Straight Through type heat shrinkable cable termination kit	Nos	Bidder to Propose as per cable schedule			
93	Diesel Generator ( Data Centre continuous rated)	Nos	2			

#	Work Detail	UOM	Qty	Unit Rate for Year 0	Tax Rate & Amount for Year 0	Total Cost for Year 0
			A	U0	T0	TC0= (U0+T0)*Q
94	HSD tank and accessories	Nos	2			
95	DG exhaust stack as manufacturer standard and compliance as per CPCB norms.	Mtr	Bidder to Propose			
96	Fuel piping with valves and accessories.	Mtr	Bidder to Propose			
97	Fuel Pump with intrinsically safe meter having feature to connect to DCIM for real time fuel consumption monitoring	Nos	Bidder to Propose			
98	Cables as per cable schedule with terminations	Lot	Bidder to Propose as per cable schedule			
99	UPS systems 2 x 400 KVA for Critical Load	Set	2			
100	UPS systems 2 x 20 KVA for Non-Critical Load with SMF batteries including battery stand		1			
101	Lithium Ion batteries for Critical load for 15 minutes back up on each UPS including battery stand.	Set	2			
102	UPS input breaker with housing for critical UPS	Nos	4			
103	UPS input breaker with housing for Non-critical UPS					
104	Battery bank breaker with housing	Nos	Bidder to Propose			
105	DC Main LT panel 1 (MLTP 1) with all associates	Nos	1			
106	DC Main LT panel 2 (MLTP 2) associates	Nos	1			
107	SDC 2.0 LT panel ( SDC LPT 2) associates	Nos	2			
108	Removal of existing DG Sync Panel, cable from DG to DG sync panel to LT panel	Lot	1			
109	DG output panel 1 (IP 66) outdoor type	Nos	1			
110	DG output panel 2 (IP 66) outdoor type	Nos	1			
111	Copper Earth pit	Nos	Bidder to Propose			
112	GI Earth Pit	Nos	Bidder to Propose			
113	Copper earth Strip with insulation	Mtr	Bidder to Propose			
114	GI Earth Strip with insulation	Mtr	Bidder to Propose			
115	Distribution Board (TPN)	Nos	Bidder to Propose			
116	Distribution Board (SPN)	Nos	Bidder to Propose			
117	Sub mains cabling	Mtr	Bidder to Propose			
118	Light and Power point Wiring	Lot	Bidder to Propose			
119	Modular switch board with switches and sockets for wall	Nos	Bidder to Propose			
120	Modular switch board with switches and sockets for Desk	Nos	Bidder to Propose			
121	MS Conduit with accessories	Mtr	Bidder to Propose			
122	PVC conduit with accessories	Mtr	Bidder to Propose			
123	Flexible MS conduit	Mtr	Bidder to Propose			
124	Flexible PVC conduit					
125	Smart LED lights Rectangular	Nos	Bidder to Propose			
126	Smart LED light Round	Nos	Bidder to Propose			
127	Smart LED Lights Square 2'x2'	Nos	Bidder to Propose			



#	Work Detail	UOM	Qty	Unit Rate for Year 0	Tax Rate & Amount for Year 0	Total Cost for Year 0
			A	U0	T0	TC0= (U0+T0)*Q
128	Smart LED lights Square 1'x1'	Nos	Bidder to Propose			
129	Occupancy sensor range 6-7 meter	Nos	Bidder to Propose			
130	NEMA (IEC 309) connectors with breaker	Nos	Bidder to Propose			
131	BUS BAR trunk from transformer to Transformer output panel with all accessories	Mtr	Bidder to Propose			
132	Track bus way ( BBT) inside Data Centre with all accessories	Mtr	Bidder to Propose			
133	Tap off box with accessories for track busway system	Nos	Bidder to Propose			
134	UPS output panel with K13 isolation transformer	Nos	2			
135	HVAC panel	Nos	2			
136	Auto transfer switch for PAC ( if required)	Nos	Bidder to Propose			
137	Industrial Socket for PAC and CAC	Nos	Bidder to Propose			
138	Equi-potential grid on DC below raise floor by 25x3 copper strip with insulation	Mtr	Bidder to Propose			
139	Perforated cable tray (factory made galvanized). Please add items for various size	Mtr	Bidder to Propose			
140	MS raceway with cover. Please add items for various size	Mtr	Bidder to Propose			
141	Ladder tray. Please add items for various size	Mtr	Bidder to Propose			
142	PVC raceway under PCC floor	Mtr	Bidder to Propose			
143	Replacement of capacitors in existing panel and making the panel operational	Lot	1			
144	Shifting capacitor panel 1 mtr backwards from its existing place for making way for new panels.	Nos	2			
145	Wall fans	Nos	6			
146	Ceiling Fan	Nos	3			
147	Single line diagram A2 size laminated	Nos	4			
148	Exhaust fan ( min 18 inch dia) with gravity damper	Nos	8			
149	Clamp meter AC, DC, with clamp side suitable to fit in 240 sqr mm single core cable	Nos	2			
150	Intelligent PDU for racks	Nos	180			
151	Battery Impedance tester	Nos	1			
152	Thermal Temperature gun	Nos	1			
153	Round bottomed fire buckets-4 Nos	Set	6			
154	shock treatment chart	Set	6			
155	Danger boards	Nos	20			
156	first aid box	Nos	2			
157	Fixing of As built Single line drawing duly laminated / framed in A1 size.	Lot	1			
158	cable route markers with necessary angle iron supports	Lot	1			
159	Temporary lighting, temporary DB, Power Supply to all service vendor for DC construction till Go-live.	Lot	1			

#	Work Detail	UOM	Qty	Unit Rate for Year 0	Tax Rate & Amount for Year 0	Total Cost for Year 0
			A	U0	T0	TC0= (U0+T0)*Q
<b>C</b>	<b>HVAC SYSTEM</b>					
160	In-row Precision Air conditioner with all accessories	Nos	Bidder to propose			
162	Front throw Precision Air conditioner for Power room - min 10 TR	Noss	4			
163	Refrigerant piping with insulation and termination	Mtr	Bidder to propose			
164	Dehumidifier water line piping with all accessories	Mtr	Bidder to propose			
165	VRV/VRF system	HP	Bidder to propose			
166	Comfort AC indoor unit	Nos	Bidder to propose			
167	Refrigerant piping for VRV/VRF system with insulation	Mtr	Bidder to propose			
168	Cold aisle containment with door and accessories	Sqr.Mtr	Bidder to propose			
169	Sliding door on one side of hot aisle	Sqr.Mtr	Bidder to propose			
170	Hot aisle containment for High density POD	Sqr.Mtr	Bidder to propose			
171	Removal and closing of AHU duct at floor	Lot	1			
<b>D</b>	<b>SAFETY, SECURITY, SURVEILLANCE AND MONITORING SYSTEM</b>					
172	Addressable fire alarm system with all accessories	Lot	1			
173	Gas based suppression system for Server Hall	Lot	1			
174	Gas passed suppression system power room	Lot	1			
175	Aspiration smoke detection system	Lot	1			
176	Close circuit tele vision (CCTV) NVR	Nos	1			
177	PTZ Camera	Nos	3			
178	Bullet fixed camera	Nos	7			
179	Dome camera	Nos	42			
180	55 inch Display screen	Nos	1			
181	Door Access control system	Lot	1			
182	Flab Barrier	Nos	2			
183	Swipe barrier	Nos	1			
184	Full height turnstile	Nos	1			
185	Baggage scanner	Nos	1			
186	Metal detector Full height	Nos	1			
187	Hand held metal detector	Nos	4			
188	Fire extinguisher	Nos	10			
189	Water leak detection system	Lot	1			
190	Rodent repellent system	Lot	1			
191	Data Centre Infrastructure Monitoring system	Lot	1			
192	Asset tracking system	Lot	1			
193	Rack access control system	Lot	1			
194	Rack humidity and temp sensor	Lot	Bidder to propose			
195	Removal of fire hydrant system from server hall	Lot	1			
196	Computers for Access control system	Nos	1			

#	Work Detail	UOM	Qty	Unit Rate for Year 0	Tax Rate & Amount for Year 0	Total Cost for Year 0
			A	U0	T0	TC0= (U0+T0)*Q
197	Computers for CCTV	Nos	1			
198	Computer for DCIM	Nos	1			
199	Data Douser	Nos	1			
200	Safety Gloves, Jacket, Boot, Goggles, Fireman's axe Etc.	Set	2			
201	Evacuation Chart	Nos	5			
202	Signage's	Nos	30			
203	Self-illumination tape	Mtr	Bidder to propose			
204	Portable oxygen cylinder with mask	Nos	2			
205	LED torch ( industrial type)	Nos	2			
206	Portable emergency light	Nos	2			
207	Visitor management system with all hardware such as Photo I card printer, Computer, camera and software etc.	Lot	1			
<b>E</b>	<b>NETWORKING SYSTEM</b>					
208	Network Rack	Nos	10			
209	Cat6A cable	Mtr	Bidder to Propose			
210	Horizontal Cable managers	Nos	Bidder to Propose			
211	Copper patch cord	Nos	Bidder to Propose			
212	Patch panel	Nos	Bidder to Propose			
213	MPO cassettes	Nos	Bidder to Propose			
214	Blanking panel (2U)	Nos	3000			
215	Cable basket min size 400mmx50mm with accessories	Mtr	200			
216	Fibre Runner with accessories for all 90 racks	Lot	1			
217	42U server Racks	Nos	80			
218	I/O module	Nos	Bidder to Propose			
219	Faceplate	Nos	Bidder to Propose			
220	fibre patch cord	Nos	Bidder to Propose			
221	Conduit with accessories	Lot	1			
222	IP EPABX	Nos	1			
223	Desk IP Phones	Nos	20			
<b>F</b>	<b>CERTIFICATION &amp; HEALTH CHECK</b>					
224	Uptime Tier-III Certification	Lot	1			
225	Half yearly health check	Half yearly	10			
226	Liaison charges for Electrical Approvals form Electrical Inspector, Fire Department, PCB, PESO and other statutory bodies of Govt. of Orissa/India ( statutory charges if any will be paid by department/ OCAC)	Lot	1			
227	ISO 9001, ISO 27001 & ISO 20000 Certification Charges	Set	1			
	Total cost in Figure					
	Total cost in words					

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1																				
2	<b>ODISHA COMPUTER APPLICATIONS CENTRE</b>																			
3	<b>OCAC-NEGP-INFRA-008-2018-20038 Dated 09.10.2020</b>																			
4	<b>Name of the Bidder</b>																			
5	<b>Cost Bid for Maintenance of Civil and Non-IT Infrastructure</b>																			
6	#	Work Detail	UOM	Qty	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Total Amount Inclusive of Taxes in 5 Years
7				Q	U1	T1	TC1= (U1+T1)* Q	U2	T2	TC2= (U2+T2)* Q	U3	T3	TC3= (U3+T3)* Q	U4	T4	TC4= (U4+T4)* Q	U5	T5	TC5= (U5+T5)*Q	TA=TC1+TC2+T C3+TC4+TC5
8	1	Operation and Maintenance of Civil & non-IT Infrastructure Work complete for 5 years	Set	1																
9	Total Cost (IN FIGURE)																			
10	Total Cost (IN WORD)																			

**ODISHA COMPUTER APPLICATIONS CENTRE**  
**OCAC-NEGP-INFRA-008-2018-20038 Dated 09.10.2020**

<b>Name of Bidder</b>	< Name of Bidder >
-----------------------	--------------------

**Price Bid for IT Equipment**

#	SITC of IT Equipment & Software	UOM	Qty	OEM / Make	Model /Part Details	Unit Rate for Year 0	Tax for Year 0	Total Amount Inclusive of Taxes (INR)
	Line Item Defined in RFP - Quote -15		Q			U0	T0	TA= (U0 + T0) * Q
<b>1</b>	<b>Server</b>							
1.1	Server Type-A	Nos.	18					
1.2	Server Type-B	Nos	30					
<b>2</b>	<b>Network</b>							
2.1	Core Switch	Nos	2					
2.2	Leaf Switch (Fiber)	Nos	26					
2.3	Leaf Switch (Copper)	Nos	4					
2.4	Core Router	Nos	2					
2.5	SDN/Fabric Controller Solution	Set	1					
2.6	Management Switch -1	Nos	11					
2.7	Management Switch -2	Nos	10					
<b>3</b>	<b>Storage</b>							
3.1	SAN Switch	Nos	2					
3.2	SAN Switch	Nos	8					
3.3	Enterprise Storage - 1 PB	Nos	1					
3.4	Tape Library Solution with Min 15 Drive	Set	1					
<b>4</b>	<b>Load Balancer</b>							
4.1	Link Load Balancer	Nos	2					
<b>5</b>	<b>Cyber Security</b>							
5.1	Next Generation Firewall	Nos	2					
5.2	AAA	Nos	2					
5.3	DDoS	Set	2					
5.4	Vulnerability Assessment Solution Licenses	Nos	512					
5.5	Anti- APT Solution	Nos	2					
5.6	DLP Solution (Licenses)	Nos	250					
<b>6</b>	<b>Cyber Security Software</b>							
6.1	Server Security solution (HIPS) Licenses	Nos	400					
6.2	Datacentre Access Management Licenses	Nos	50					
6.3	Endpoint Point Security Solution Licenses	Nos	50					
<b>7</b>	<b>On Premise Services (VM Based)</b>							
7.1	EMS Management System	Set	1					
7.2	Cloud Management & Orchestration	Set	1					
7.3	Automation Software (Instance Based)	Set	1					
7.4	PaaS	Set	1					
<b>8</b>	<b>Software/License with SA &amp; Support (till project completion i.e.5 Yrs from FAT)</b>							
8.1	MS Windows Server Standard Latest Edition 16 Core License	Nos	100					
8.2	Red Hat Enterprise Linux 2 Core Latest Edition	Nos	30					
8.3	MS SQL Enterprise Database Server Latest Edition - 32 Core	Set	1					
8.4	My SQL Enterprise DB Server Latest Edition - 32 Core	Set	1					
8.5	EDB post gre Enterprise Server Latest Edition - 32 Core	Set	1					
8.6	Virtualization Software (For Cloud Servers)	Set						
<b>9</b>	<b>Desktop / Laptop/ Printer</b>							

#	SITC of IT Equipment & Software	UOM	Qty	OEM / Make	Model /Part Details	Unit Rate for Year 0	Tax for Year 0	Total Amount Inclusive of Taxes (INR)
	Line Item Defined in RFP - Quote -15		Q			U0	T0	TA= (U0 + T0) * Q
9.1	Desktop	Nos	35					
9.2	Multifunctional Printer	Nos	2					
9.3	Laptop	Nos	6					
<b>Total Cost (IN FIGURE)</b>								
<b>Total Cost (IN WORDS)</b>								



**ODISHA COMPUTER APPLICATIONS CENTRE**

**OCAC-NEGP-INFRA-008-2018-20038 Dated 09.10.2020**

**Name of the Bidder**

<Name of the Bidder>

**Cost Bid for Resources required for O&M of OSDC 2.0**

#	Resource Description	Qty	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Unit Rate for one Year	Tax for One Year	Total Cost for Year	Total Amount Inclusive of Taxes in 5 Years
	Line Item Defined in RFP Quote -19	Q	U1	T1	TC1= (U1+T1)* Q	U2	T2	TC2= (U2+T2)* Q	U3	T3	TC3= (U3+T3)*Q	U4	T4	TC4= (U4+T4)*Q	U5	T5	TC5= (U5+T5)* Q	TA=TC1+TC2+ TC3+TC4+TC5
1	DC Project Manager	1																
2	Network & Security Administrator	1																
3	Cloud & Server Administrator	1																
4	EMS Specialist	1																
5	Database Administrator	1																
6	Storage and Backup Specialist	1																
7	SIEM Analyst	1																
8	Network Engineer	4																
9	Server Engineer	4																
10	Helpdesk Support	4																
11	Facility Manager	1																
12	BMS /DCIM Expert	4																
13	Electrical Supervisor	1																
14	Electrical Technician	4																
15	Housekeeping Staff	2																
16	Back office Staff	2																
17	Security Guard	8																
18	Front Desk Executive	1																
Total Cost (IN FIGURE)																		

Please Note:-  
 1. Above Manpower requirement sheet is indicative as minimum requirement, bidder should have a clear prospective of the requirement of manpower to maintain this project and achieve the required SLA. Bidder should have their spare resource to meet the challenge of leave/replacement/changes.



**ODISHA COMPUTER APPLICATIONS CENTRE**

**OCAC-NEGP-INFRA-008-2018-20038 Dated 09.10.2020**

**Name of Bidder**

**Buyback Price for Existing equipment at SDC**

<b>S. No.</b>	<b>Equipment</b>	<b>Quantity</b>	<b>Buyback Price/Per Unit</b>	<b>Total Buyback Amount</b>
		<b>Q</b>	<b>U</b>	<b>TA= Q*U</b>
1	Buyback of SDC Hardware after migration of all applications and shifting of required sufficient equipments	1		
<b>Total Cost (IN FIGURE)</b>				
<b>Total Cost (IN WORDS)</b>				

Proposed Integrated Network Diagram (Indicative)

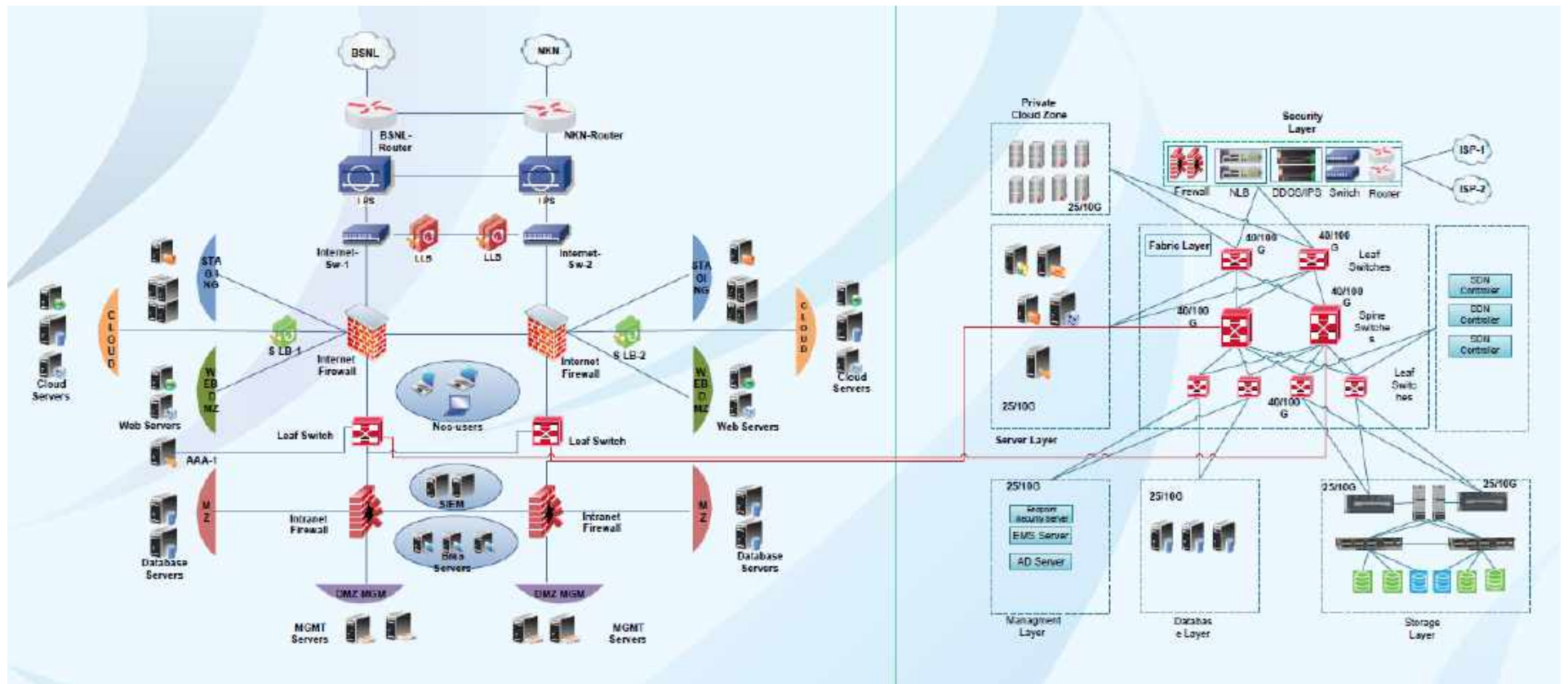


Fig. No-22

Proposed Broad Architecture of the cloud enabled Data Centre

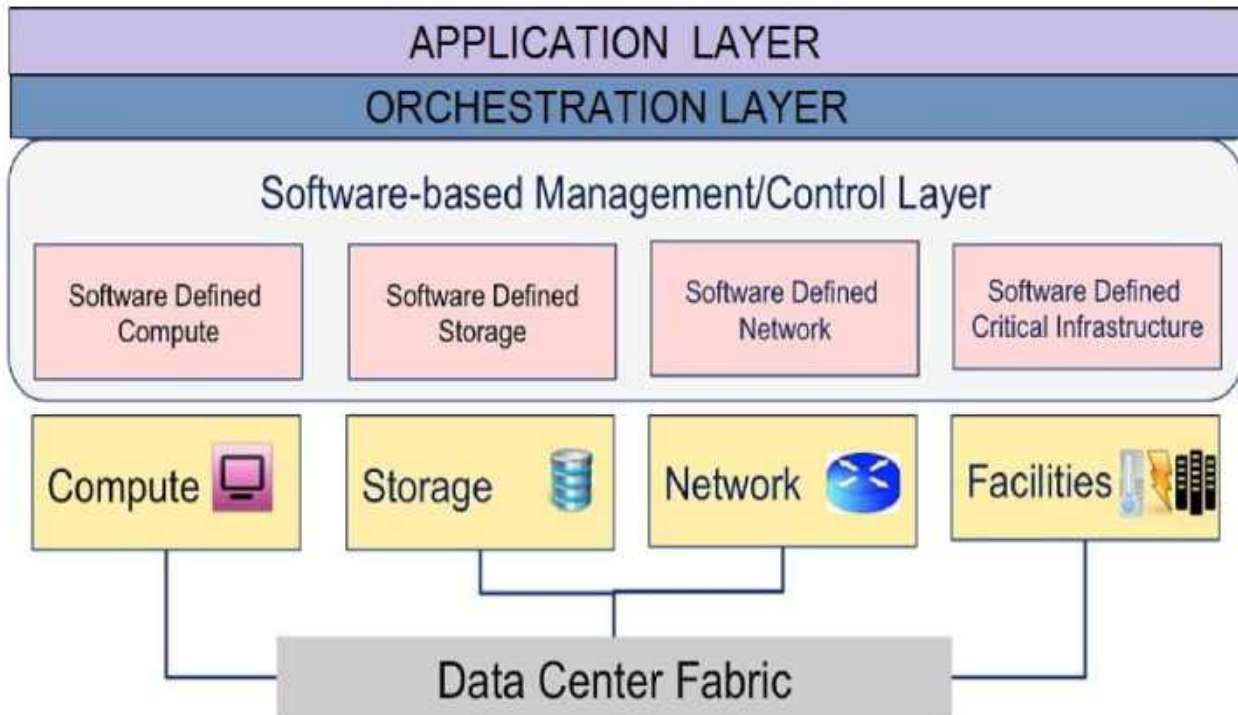


Fig. No-23

## 6.6. IT Infrastructure (Scope of Work)

The overall Scope of Work (SoW) for the Bidder to be appointed through this RFP for the IT Infrastructure includes the following but not limited to:

### 6.6.1 Detailed Functional Scope of Work

The Bidder shall adopt fabric-based approach that is designed from the foundation to support emerging industry demands. To allows both traditional enterprise applications and internally developed applications to run side by side on a network infrastructure designed to support them in a dynamic and scalable way. Network policies and logical topologies, to be applied based on the application needs. DC Architecture should have Network fabric design with Spine & Leaf model design to support the move to management automation, programmatically defined policy, and dynamic workloads of both Virtual & physical device.

Next Generation OSDC 2.0 should help OCAC to achieve the following functional requirements:

- i. **Rapid service provisioning:** Services must be available in the shortest time possible. Administrative and bureaucratic efforts to introduce applications can be minimized. The major offerings to the various Government Departments would be in the form of a Private Government cloud running on one or multiple of the established Hypervisors.
- ii. **Cyber Security:** Security is one of the biggest concerns and is required by regulation. Standard tasks like firewall configurations demand a lot of effort. Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc. Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, and Denial of Service. Data Centre Architecture should provide secure zero-trust using whitelist policy model in a heterogeneous network environment
- iii. **Consistent services and manageability on physical devices and virtual overlays:** Design should support Virtualization from one or more vendors. Consistency in terms of manageability, troubleshooting, and security must be present between different virtual networks and the physical network to help minimize the administrative efforts and eliminate errors.
- iv. **Multi-vendor service integration:** Data Centre should have built on the technologies of multiple vendors. It must be verified that infrastructure components (like security, load balancing, virtualization, and storage) from various vendors operate together.

**Network Fabric:** The proposed network fabric shall be of a two-trier design architecture adaptable to the continuously changing needs within the enterprise Data Centre. The network would gradually move to Software defined Networking with Leaf and Spine architecture which would give better utilization of the switching fabric. The existing DC and the proposed new DC will be linked through a dark fiber for network manageability and pose as a single network. The network aggregation layers will have having 40 Gb bandwidth, and the rest will be on a 10 Gb backbone. The access layer consists of leaf switches that connect to devices like servers, firewalls, load balancers, and edge routers whereas the core layer would be the backbone of the network. Network Fabric should have the core and access layer architecture. Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud

automation & Orchestration software. Bidder has to own the responsibility of making the solution run as desired by OCAC. Bidder to implement the network and post successful run, has to handover the active part to OCAC. The design should support for deployments that start small, but then grow to large-scale over time, while sticking to the same overall architecture. The solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.). Solution should integrate seamlessly with customer's existing network infrastructure make router/switches/firewalls/IPS and various types of WAN links. Solution shall contain list of all features provided by each component of the proposed solution in addition to the specifications mentioned in this document that will be available to the customer without any additional charges and will be under support. These features will be treated at par with other features mentioned in the RFP. Solution should have license without any restrictions to use the features mentioned in the RFP from day one. If during the contract, solution is not performing as per specifications in this RFP, bidder has to upgrade/enhance the devices or place additional devices and reconfigure the system without any cost to OCAC. All required optical transceivers, Direct-Attach-Cables etc. shall be from the same hardware OEM. No third party components shall be allowed. Selected SI has to fully populate the asked SFP/SFP+/QSFP+/FC ports as per RFP and corrigendum with complete optical transceivers as per their solution design including all additional items, as would be needed for overall solution completeness. All optical transceivers shall have LC interfaces suitable for MMF duplex fiber cabling inside the SDC.

- v. Compute: SDC intends to have high-density compute setup comprising of next-generation rack servers that can be deployed as "Anything-as-a-service" wherein each such server can be a 2-processor based. Solution should be capable of adding high performance processors (usually exceeding 150W) along with high performance GPU capabilities to scale performance and capacity on demand. Current SDC has 4500 (approx.) compute core and 500 TB of Storage. These infrastructure solution will be the part of the OSDC 2.0. Currently, the Core compute is virtualized with the Hyper-V & VMware platform license and support. Bidder needs to ensure for migration of the same platform in the OSDC 2.0, and it should be part of the bidders proposed solution. Bidder will have to create the parallel staging environment of required provisioned core size as per specified in the OSDC 2.0 BoQ core size and it should be physical & virtually in different zone. Any access to pre-production environment should be completely differ from the production environment (different security measures). The proposed Server Type- B has been provisioned to provide the cloud services. Bidder has to proposed detailed bill of quantity for the provisioned 30 cloud servers as per their design and solution proposed.
- vi. SDN controller: SDN ready infrastructure shall be deployed to configure and build physical networking infrastructure with Spine and leaf switches. These high end data Centre switches should have the flexibility to support SDN capabilities such as VXLAN, MP-BGP, etc. and have the ability to get configured from a centralized station such as management and orchestration software entity in addition to being able to be deployed in the traditional/standalone mode. DC Fabric must provide open scripting interface from the central management appliance / SDN Controller for configuring the entire fabric. Centralized management appliance or SDN Controller must communicate to south bound devices using open standard protocol.

- vii. **Visibility:** Fabric must provide deeper visibility into the fabric in terms of latency/packet drop between VM to VM, VM to Physical server and vice versa, access to another access etc. Should provide pervasive visibility of traffic across the entire data centre infrastructure, including servers. Should provide complete visibility into application components, communications, and dependencies to enable implementation of a zero-trust model/micro segmentation in the network.
- viii. **Virtualization:** SDC Fabric must integrate with minimum 2 Virtual Machine Manager (i.e. v-Centre, SCVMM, OpenStack etc.) of different Hypervisors like VMware, Hyper-V, KVM, Xen etc. simultaneously. Bidder will have to propose the compatible Virtual Machine Manager which must be integrated with the integrated with proposed SDC fabric.

**Next-Generation Data Centre Security:** SDC Security architecture should have support for network virtualization and enable Layer 4 through 7 virtual network service chaining for security by using an application-centric, unified, and automated approach to security policies in the data Centre infrastructure that is decoupled from the underlying network topology, supports application mobility, offers real-time compliance lifecycle management, and reduces the risk of security breaches. Solution should automate and centrally manages security policies in the context of an application using a unified security policy abstraction model that works across both physical and virtual boundaries. Should Support for Geo-location, dynamic policy creation, deletion, migration, and line-rate enforcement is needed to secure east-west traffic and properly manage application mobility. SDC architecture should provide threat-focused Next-Generation Firewall, IPS with best of breed industry leading stateful firewall with the best of breed threat capabilities such as next-generation intrusion prevention and Advanced Malware Protection, URL filtering (web scanning), application control. Get granular application control. Protect against malware. Gain insight into and control over threats and vulnerabilities.

- a. **Application Visibility and control:** Identify and control user access to over thousands commercial applications, plus support custom applications.
- b. **Next Gen Intrusion Prevention System:** Get the visibility, automation, flexibility, and scalability you need to defeat the latest threats.
- c. **Advance Malware Protection:** Discover, track, contain, and block the progression of network-based advanced malware, zero-day attacks, and persistent threats. Supported application protocols like HTTP, SMTP, IMAP, POP3, FTP etc.
- d. **URL Filtering:** Get alerts and gain control over suspect web traffic. Enforce policies on millions and millions of URLs in lot many different relevant categories
- e. **Web Application Firewall:** Should protect against application layer attacks targeted at web applications. Should provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting and support OWASP application security Methodology.

- ix. SAN Switching: The SAN solution should offer highly predictable performance, scalability, Intelligence, and ease of management while protecting customer investment. The proposed switches should provide a best-of-breed solution that can work in multi-protocol FC, FCoE, and IP storage (Internet Small Computer System Interface [iSCSI], VSAN and FC over IP [FCIP]) environments.
- x. Storage Infrastructure: Centralized storage with flexible and secure configuration shall be available in the SDC including backup facilities. The same shall be leveraged by different line departments for their data storage requirements in shared manner.
- xi. Structured Cabling: Bidder has to design, lay and test the cabling to cater approx. 90 racks of SDC. The bidder to provide the best of breed solution to manage end to end connectivity (both server rack and backbone/uplink connectivity for DC) and backbone between Spine and Leaf switches, SAN switches and access switches to server rack will be on multimode OM4 fibre. All the work shall be done in a conscientious manner as per the OEM guidelines and best industry practices.
- xii. Enterprise Management System: EMS Software solution overview should clearly articulate the technical approach of the infrastructure solution implementation. This proposed solution should meet the EMS requirements for OSDC 2.0. The EMS solution consists of a unified dashboard for infrastructure performance, event consolidation and correlation, server and database performance management, end to end network fault and performance management and automation, Help Desk, Patch automation for the entire infrastructure and integration with Privileged Access Management. The proposed solutions should drive efficient change, automated configuration, security administration, and compliance. The EMS system should provide for the regular monitoring, management and reporting of the IT infrastructure of the OSDC. The proposed solution should have a single-point-of-contact IT Help desk software that should use a consistent set of automated processes to quickly and efficiently handle service delivery and support. The proposed service management system should provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs
- xiii. Cloud Infrastructure: OCAC has a vision to transform its SDC into a state of the art " Private Cloud" with Agile infrastructure, supporting new age application requirements, seamless scale with Self Service consumption and enhanced security/governance, at the same time ensuring to utilize the existing investments to its fullest. As part of OSDC 2.0, to build a common secure cloud Management platform with IaaS, PaaS, SaaS, DbaaS, Bare Metal as a service and CaaS capabilities for SDC 2.0.

To get the most out of the existing investments by reusing existing infrastructure up to the extent possible, integrating with existing platform under common cloud management layer. The cloud services can be initiated with basic Compute Services (CPU, RAM, Storage, OS, and database) to the departments on demand basis along with a Production and Staging environment. Once OSDC develop confidence/maturity in operating cloud enabled environment, gradual migration of existing infrastructure and applications shall happen on OCAC cloud.

The digital transformation architecture design principles of OSDC is given below in the illustrative figure:

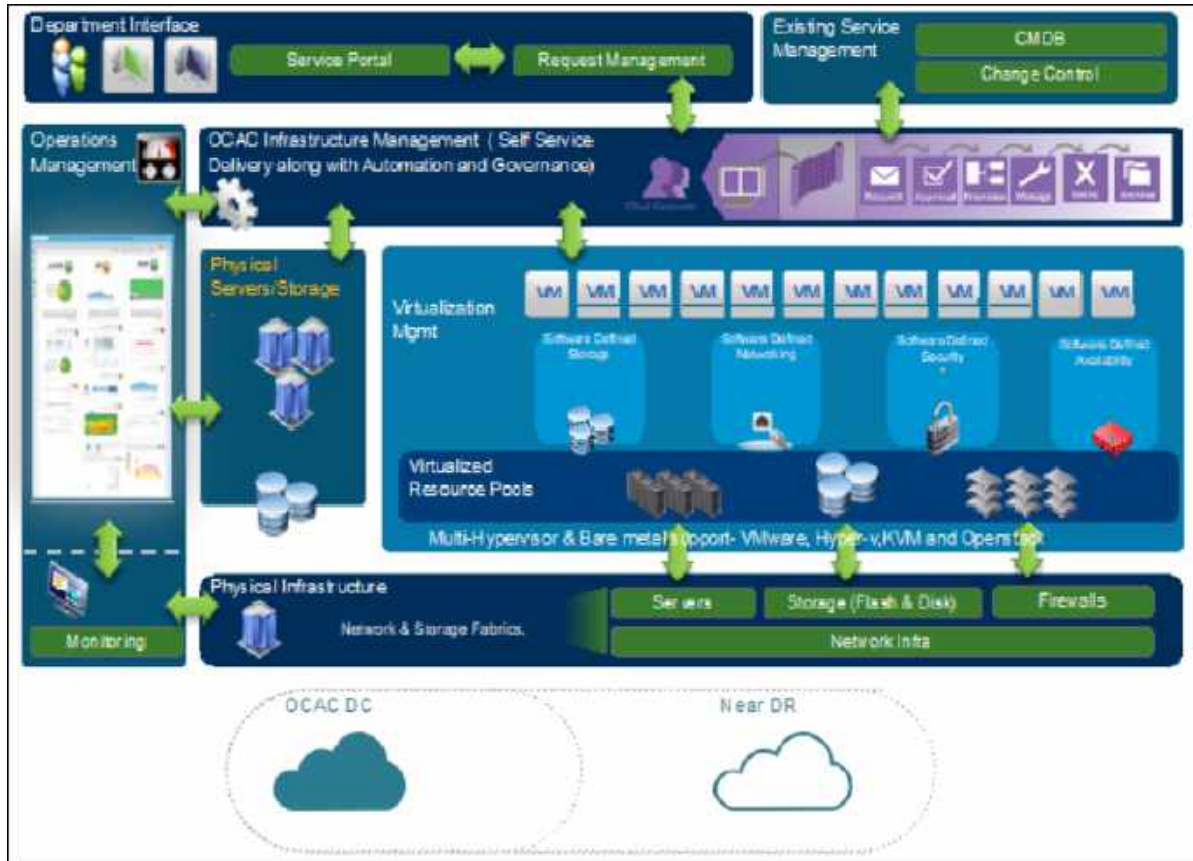


Fig. No-24

- xiv. High Level Scope of Cloud: The proposed cloud solution must support & integrate with existing VMware Cloud Management Platform & Network Virtualization solution currently deployed at OSDC.

The bidder shall supply Hardware, Software and services as per schedule of Requirements and in accordance with minimum **functional & technical specifications** as provided in the below sections.

Design and Implementation of the private Cloud with underlying software components (virtualization, SDN, container, security, storage etc.) should be done by OEM certified professionals. Training should also be provided by OEM certified trainer on all the above cloud technologies aligned with the SDC team’s requirement.

The ability to maintain a common set of templates across all department is a strict requirement of OCAC which aims to reduce the number of blueprints requiring creation and management



- Solution should be deployed to create customized workflows as per requirement with IaaS, PaaS, SaaS, DbaaS, STaaS, Back up as a service, Bare Metal as a service and CaaS capabilities for SDC 2.0 as defined in functional requirements and services scope.
- Any required version/Software /Hardware upgrades, patch management at the new DC will be supported by the Bidder for the entire contract period
- Bidder should supply OS, database or other licenses required for Cloud management components.
- Solution should provide multi-tenant environment capabilities.
- Solution should provide automated delivery of IaaS, PaaS, SaaS, DbaaS, STaaS, Back up as a service, Bare Metal as a service and CaaS capabilities for SDC 2.0 as a service without any manual intervention.
- The proposed Cloud platform must support and manage cloud services across multiple Hypervisors (Esxi, Hyper-V, Xen, RHEV, KVM, etc.), and heterogeneous compute, heterogeneous storage & heterogeneous network.
- Solution should be configured to provide auto scale – for example increase/decrease in utilization additional VMs should be automatically be created with all network, security and load balancing assigned.
- All integration from cloud portal, orchestration, virtualization, virtual network, security and load balancing should be done to achieve full automation.
- The Solution Should support Open standards & should be interoperable with Open Stack technologies
- The proposed solution must support Hybrid Cloud mode where cloud services could be extended into a public & Meity empaneled cloud provider with single pane of glass management and mass migration of workloads without any downtime across private and public cloud.
- Solution must have cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc.
- Solution should monitor utilization of running VMs, Containers and should reclaim resources from idle VMs and allocate to other VMs in automated fashion.
- Solution should have prebuilt and configurable operations dashboards to provide real-time insight into Cloud infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements.
- The Solution shall be capable of automating security to achieve micro segmentation and zero trust security along with workload provisioning.
- Integration of existing/New AD/LDAP with cloud management platform.
- Setting of different user and administrator level permissions.
- Solution should able to define roles and limit management scope based on location, function, application, zone, life cycle, VM content, and any user defined criteria.
- Solution should be capable of network, security, storage and Configuration Policies automatically during cloud instance Provisioning
- Solution must support and provide automated compute, network, and storage for containers and automate the deployment of Container orchestration along with its networking and security.
- Solution must support and provide automated compute, network, and storage for containers and automate the deployment of Kubernetes orchestration along with its networking and security.
- The offered solution should have kernel level security deployment for offered container platform.
- The offered solution should have built in container scanner for security content automation for the container layer.
- The offered CaaS solution should be offered with integrated service mesh for microservices deployment.
- The offered CaaS solution should be offered with integrated container runtime and container build capabilities.

- The offered CaaS solution should be deployed in physical server as bare metal deployment.
  - The offered CaaS solution should include developer productivity tool like IDE, Dev Metrics, Dev logging, Packaging, Service catalog, runtimes etc.
  - The proposed solution should have the capability of providing approvals and customized integrated workflows.
  - 
  - The proposed cloud solution should provide capability of modifying cost and adding additional cost drivers.
  - The proposed cloud solution should have capability of assigning costs of individual services provided by the OCAC Service catalogue.
- xv. **Orchestration Layer:** A strong multi-cloud architecture including support for a range of MeitY approved public and private cloud platforms. Should support Software Defined Networking, Policy-based orchestration with strong API support, Life Cycle Management workflows Provisioning, Decommissioning , Extensible Capabilities to allow “Self-Management” ,workflows (Reboot/restart, Migrate, Upgrade etc.). Should support Multitenancy and User Management On-demand, self-service provisioning portal through which users can access infrastructure services or the infrastructure needed to support platform stacks being provisioned. Automated creation of virtual and physical instances and assignment of virtual infrastructure through appropriate tooling to support end-to-end automated provisioning, bare metal provisioning should be provided. Integrated usage tracking functionality to support departmental bill-back / show-back. It also should provide REST base APIs and full API-level access to all functional components of the compute service such that any function available through the user interface is available through a REST API. It also should provide Role-based policy management, administration, configure and enforce role based policies.
- xvi. **Patch Management:** The Bidder will be required to provide services related to Patch Management that will help in the evaluation of threats posed by known vulnerabilities, assign a risk factor to them and also test the patch before deployment. The patch management solution should be executed efficiently for all kinds of environments like for operating systems and Data bases.
- xvii. **Enterprise Management System (EMS):** The EMS system should provide for the regular monitoring, management and reporting of the IT infrastructure of the SDC. The EMS system must have the following features including but not limited to: Following functionalities are desired by use of such EMS tools:
- a. Availability Monitoring, Management and Reporting for compute and networking.
  - b. Performance Monitoring, Management and Reporting compute and networking.
  - c. Securing critical servers using Server based Access Control & recording user activity through audit logs.
- xviii. **Vulnerability Assessment:** The Bidder shall be responsible for various assessment as well as investigation activities basis various cyber-security guidelines as applicable and as per OCAC guidelines. Vulnerability assessment will cover the following the activities, but not limited to:
- a. Web Application based vulnerability assessment: Evaluation of security vulnerabilities associated with web applications – Apache, IIS, Tomcat, etc., thereby, recommend solutions to problems.

- b. OS level vulnerability assessment: Evaluation of security vulnerabilities associated with operating systems – Unix, Linux, Sun OS, Windows, etc., thereby, recommend solutions to problems.
- c. Database vulnerability assessment: Evaluation of security vulnerabilities associated with database –Microsoft SQL Server, MySQL, Oracle, DB2, etc., thereby, recommend solutions to problems.
- d. Network level vulnerability assessment: Evaluation of security vulnerabilities associated with Network components – Routers, Firewall, etc.,

Vulnerability Assessment will include checks like Port scan, unnecessary or vulnerable services, file permission, user access control, password protection, system vulnerability Firmware vulnerabilities, etc.

- xix. Penetration Testing: The Penetration Testing will include activities to identify specific exploitable vulnerabilities and expose potential entryways to vital or sensitive data. The results should clearly articulate security issues and recommendations and create a compelling event for the entire management team to support a security program. Must be perform one time before Go-Live and report needs to close all observation. VA and PT must be perform at regular interval of every QGR.
- xx. Server security (HIPS) deployment with management console. Regular update and policy need to update. For the endpoint security need to deploy for the Desktop and Laptop along with Management console.
- xxi. Backup Software: The Bidder shall be responsible for backup of storage as per the policies of OCAC basis mutual discussions at the time of installation and configuration. Bidder shall be responsible for:
  - a. Monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to related retention policies.
  - b. Prompt execution of on-demand backups of volumes and files whenever required by OCAC or in case of upgrades and configuration changes to the system.
  - c. Real-time monitoring, log maintenance and reporting of backup status on a regular basis.
  - d. Prompt problem resolution in case of failures in the backup processes.
  - e. Undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite).
  - f. 24 x 7 support for file and volume restoration requests at the Data Centre.
- xxii. OS Hardening: OS Hardening will include activities but not limited to the removal of all non-essential tools, utilities, and services with other system administration by activating & configuring all appropriate security features. The entire scope of this service will differ on different Operating System basis. Most of the Windows based Operating Systems will include following activities under guidance of OCAC. Broad categories of such activities are:
  - a. Identifying unused or unnecessary ports.
  - b. Disable/Shut down/remove unused and unnecessary services and daemons.
  - c. Removing rogue connections
  - d. Setting up filters for malicious content for each OS.

- e. Test Backup and restoring procedures.
- f. Account Policies: Password policy, Account lockout policy etc.
- g. Local server Policies: Audit policies, User rights assignments, security options etc.
- h. Event logs settings
- i. System services
- j. Registry settings
- k. File & Folder permissions

#### 6.6.2 Design Validation and Change

The successful Bidder would be required to prepare detailed deployment design document (both physical and IT) and shall submit the same for approval within 2 weeks from the signing of the contract Agreement with OCAC. However a Solution design has to be provided during the bid process. While preparing the design the Successful Bidder shall keep in mind the existing DC set up in the 2<sup>nd</sup> Floor of OCAC Building in terms of scalability requirements and shall plan for less downtime during the implementation.

#### 6.6.3 Installation and Configuration of the Commissioned IT Infrastructure

The successful Bidder would be required to undertake pre-installation planning at the SDC including but not limited to civil design, Construction, Interiors, Rack planning, structured cabling, SAN cabling, power points, etc.

- a. The Bidder shall be responsible for the delivery, installation testing and commissioning of the servers, storage, network, security, cloud orchestration, EMS and related equipment in the Data Centre.
- b. The Bidder shall carry out the planning and layout design for the placement of equipment in the provisioned Data Centre. The plan and layout design should be developed in a manner so as to optimally and efficiently use the resources and facilities being provisioned at the Data Centre.
- c. The plan and design documents thus developed shall be submitted to OCAC for approval and the acceptance would be obtained prior to commencement of installation.
- d. The Bidder shall carry out installation of equipment in accordance with plans and layout design as approved by OCAC.

#### 6.6.4 Deployment Phase

- a. Bidder should be involved in Planning, Designing, and final acceptance to make sure that proposed solution should work seamlessly as per tender requirement. The SI shall procure the materials and equipment as required and given as part of the SI's response. However, it should be noted that the SI is expected to procure all necessary equipment to install the requirement in the proposed expansion set up. In case, it is identified that certain components are required for required functionality but not included in the Tender BOQ , SI should include such equipment in the bid value , quote for them as "others or miscellaneous " including a list for the same with individual item description, unit cost .

- b. The seamless integration of all IT and Non-IT devices would be the bidder's responsibility holistically. Although IT -device OEM's professional services for integration and upgradation should be added for best utilisation of these devices.
- c. After successful commissioning and FAT completions of the project, bidder to ensure complete handover and knowledge transfer from OEMs for operations and management.
- d. The seamless integration of all IT and Non-IT devices would be the bidder's responsibility holistically. Although IT -device OEM's professional services for integration and upgradation should be added for best utilisation of these devices.

#### 6.6.5 Procurement & Delivery of IT infrastructure components

The Bidder shall procure and supply all components and sub components (Active as well as passive), as per requirements of the RFP/Contract. The Bidder shall be responsible for supply/ installation of:

- All active and passive components required for the expansion area of server farm of Odisha State Data Centre
- IT Infrastructure components such as Storage, Networking & Security components and other IT components required at the Data Centre

The SI will be responsible for delivering the equipment at the data Centre site. The SI shall supply all the installation material/ accessories/ consumables (e.g. screws, clamps, fasteners, ties anchors, supports, grounding strips, wires etc.) necessary for the installation of the systems.

The SI has to prepare and submit a delivery report including details of all components supplied. The delivery report will be validated by the OCAC.

Any additional equipment procured by Bidder, will be supplied by the respective OEM. The Bidder would be responsible for inventory check, testing and installation of the equipment accordingly and coordinating with the supplier as required.

The Scope of Work consists of the Procurement of various IT components required for the implementation of the Solutions as follows but not limited to as mentioned in Bill of Quantity:

S. No.	Item Description	UoM	Quantity

Bill of quantities are indicative mention and the purchaser reserves the right at the time of award of contract to increase or decrease the quantity of goods and / or services from what was originally specified while floating the RFP without any change in unit price or any other terms and conditions.

### 6.6.6 Implementation

Bidder shall provide a complete data Centre solution to OCAC as a part of their technical bid. Any activity not mentioned here but required for the implementation of data Centre shall be taken in note.

The solution provided by the Successful Bidder shall meet all the service level requirements. While the basic bill of material will not change, any change in the basic BOM will be done in consultation with the SIA. It is recommended that the Bidder should thoroughly go through the RFP, to adhere to the service levels as mentioned in the document.

- a. Bidder shall be responsible for complete management of the project as per RFP T&C.
- b. Bidder to ensure that the entire infrastructure is supported back to back by respective OEM's support services.

**Solution Capability:** The professional experts from the OEM team are expected to support in periodic reviews during the project timeline to ensure that capabilities of the proposed infrastructure are deployed effectively. The reviews are expected to take place at the following stages of the project implementation.

- Technical Solution Preparation
- Solution Implementation
- Final Preparation for Go-Live
- Stabilization period
- Final Go Live.

### 6.6.7 Migration to OSDC 2.0

The Bidder is expected to carry out all the activities pertaining to migration of the existing SDC infrastructure to the planned OSDC 2.0.

- a. Data migration from existing storage to new storage under the guidelines of OCAC.
- b. Application migration in coordination with application owners / departments and under the guidelines of OCAC.
- c. Migration of Servers, network and security stack and other necessary items based on business requirement with minimal downtime as possible.
- d. The scope of Bidder is only the migration and management of the physical Infrastructure and also provides facilitation to the Application owner. Application will be migrated by individual application owner.
- e. The Bidder shall have to ensure that required dependencies along with their associated items are met and/or are included in their solution for the said application migration to OSDC 2.0. However, Application enhancement will not be the responsibility of the Bidder. However, bidder will not be charged any penalty in case of any delay in the readiness of the application.
- f. Existing cloud Infrastructure solution of SDC needs to be migrate from existing SDC to OSDC 2.0, including shifting of the hardware.

- g. Bidder should provide approach and methodology to migrate infrastructure solution and application from SDC to OSDC 2.0.
- h. Bidder shall envisage implementing the IPv6 enablement. The existing SI/DCO will support in implementing IPV6 implementation during the migration process.

## 6.7. Operations & Maintenance

Following are the summary of operations and maintenance services to be provided by the Bidder to be performed under the supervision of OCAC. OCAC will finalize quantities of the resources and confirm to bidder in form of purchase order and Bidder has to deploy all ordered onsite resources (as per purchase order) for Data Centre operation and maintenance on or before the date of Go-Live of the solution.

- a. Bidder should ensure that a robust support model as per the indicative manpower planning table, in such a way that the data Centre runs with the level of availability it is designed for and with a predictable restoration time in case of any failure.
- b. Once deployed, the bidder is completely responsible to manage the entire support model to ensure the SLA uptime.
- c. Bidder shall provide comprehensive onsite support on 24 x 7 x 365 basis to ensure an uptime of 99.982% for the IT infrastructure solution at the Data Centre in accordance with the Service Level Agreement mentioned as part of this tender.
- d. Bidder shall commit to provide all necessary manpower resources onsite to resolve any issues/incidents and carry out required changes, optimizations and modification.
- e. Bidder shall assign onsite manpower resources on 24 x 7 x 365 basis to diagnose, troubleshoot and resolve issues related to the Data Centre services. The onsite support staff should possess capability for supporting the equipment and components proposed, but not limited to undertaking preventive and break-fix maintenance, troubleshooting, resolving problems, tuning, etc. Bidder shall also provision for necessary offsite support to ensure continuity of operations for OSDC 2.0.
- f. Bidder shall provide comprehensive technical support services for all the hardware and software proposed for the entire period of the contract. The technical support should include all the upgrades, updates and patches that are released by the respective OEMs during the period of contract.
- g. Bidder shall provide comprehensive onsite warranty on 24 x 7 x 365 basis for a period of 5 (Five) years from the date of Go-Live of all IT infrastructure provided as part of scope of this tender. The warranty period shall commence from the date of acceptance of the entire system only.

### 6.7.1 Onsite Support

The Bidder should ensure that the entire IT Infrastructure solution is operational in accordance with the stipulated service standards in Service Level Agreement.

The Bidder along with all of their associated OEMs should commit to provide all necessary resources and expertise to resolve any issues and carry out required changes, optimizations and

modification to ensure that the IT infrastructure is operational in accordance with the stipulated service standards in Service Level Agreement.

- a. The Bidder should provide comprehensive onsite warranty on a 24x7x365 basis for a period of 5 (Five) years from the date of Go-Live of all IT infrastructure solution provided as part of scope of work. The warranty period shall commence from the date of acceptance of the entire system as described in RFP.
- b. The onsite technical support should also include all the upgrades, updates, major or minor patches that are released by the respective OEMs during the period of contract.

### 6.7.2 Technical Support

The onsite Technical team will coordinate OCAC technical support desk for the resolution of all IT infrastructure related issues / problems. OCAC Technical Support desk shall undertake the following activities:

- a. Log issues / complaints related to IT infrastructure at the Data Centre and issue an ID number against the issue / complaint.
- b. Assign severity level to each issue / complaint so as to maintain categorization and differentiate the criticality of the incident via the priority levels, severity levels and impact levels
- c. Track each issue / complaint to resolution.
- d. Escalate the issues / complaints, to OCAC officials if necessary as per the escalation matrix defined in discussion with OCAC.
- e. Analyse the issue / complaint statistics and bidder's SLA
- f. Should provision for all necessary channels for reporting issues to onsite technical team. The incident reporting channels will be the following:
  - Email
  - Telephone (mobile phone alerts)
  - Web Based
- g. Should implement a call logging system in line with the severity levels as mentioned in the SLA.

### 6.7.3 System Maintenance and Management

Certain minimum deliverables sought from the Bidder with regards to System Maintenance and Management are provided below:

- a. The Bidder shall be responsible for tasks including but not limited to setting up servers, configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary. It should be noted that the activities performed by the bidder will be under the supervision of OCAC.
- b. The Bidder shall provision skilled and experienced manpower resources to administer and manage the entire IT Infrastructure solution for OSDC 2.0.



- c. On an ongoing basis, the bidder shall be responsible for troubleshooting issues in the IT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.
- d. The Bidder shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.
- e. The Bidder shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with OCAC and based on the industry best practices / frameworks. The Bidder shall also create and maintain adequate documentation / checklists for the same.
- f. The Bidder shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc.
- g. The Bidder shall be responsible for management of passwords for all relevant components and devices under his purview and implement a password change mechanism in accordance with the security policy formulated in discussion with OCAC and based on the industry best practices / frameworks like ISO 27001:2013, ISO 20000:2011, ISO 9001:2013.
- h. The administrators will also be required to have experience in latest technologies like Orchestration, virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario.

#### 6.7.4 System Administration

Certain minimum deliverables sought from the Bidder with regards to System Administration are provided below:

- a. 24\*7\*365 monitoring and management of the servers in the Data Centre.
- b. The Bidder shall ensure proper configuration of server parameters. The Bidder shall be the single point of accountability for all hardware maintenance and support the IT infrastructure at the Data Centre.
- c. The Bidder shall be responsible for Operating system administration, including but not limited to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.
- d. The Bidder shall also be responsible for installation and re-installation in the event of system crash/failures.
- e. The Bidder shall appoint system administrators to regularly monitor and maintain a log of the monitored servers to ensure their availability to OCAC at all times.
- f. The Bidder shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log analysis. The system administrators should also ensure that the logs are backed up and truncated at regular intervals. The bidders are advised to refer CERT-In Guidelines so as to ensure their alignment with the practices followed.
- g. The system administrators should adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.
- h. The system administrators should provide hardening of servers in line with the defined security policies

- i. The system administrators should provide integration and user support on all supported servers, data storage systems etc.
- j. The system administrators should provide directory services such as local LDAP services and DNS services and user support on all supported servers, data storage systems etc.
- k. The system administrators will be required to trouble shoot problems with web services, application software, desktop/server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.
- l. Documentation regarding configuration of all servers, IT Infrastructure etc. The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.
- m. The administrators will also be required to have experience in latest technologies like Orchestration, virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario.

#### 6.7.5 Storage Administration

Certain minimum deliverables sought from the bidder with regards to Storage Administration are provided below:

- a. The Bidder shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN fabric / switches, Virtual tape library, etc.
- b. The Bidder shall be responsible for storage management, including but not limited to management of space, SAN volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.
- c. OCAC would additionally remotely manage the storage system and components and appropriate setup should be provided by the Bidder
- d. The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.
- e. The storage administrator will be required to create/delete, enable/disable zones in the storage solution
- f. The storage administrator will be required to create/delete/modify storage volumes in the storage solution
- g. The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution
- h. To facilitate scalability of solution wherever required.
- i. The administrators will also be required to have experience in latest technologies like virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario.

### 6.7.6 Database Administration

Under the supervision/ guidance of OCAC, the Bidder shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.

- a. The Bidder shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.
- b. The Bidder shall be responsible for tuning of the relational database, ensuring the integrity of the data and configuring the data dictionary.
- c. The Bidder shall be responsible for testing and installing new database software releases, if any.

### 6.7.7 Backup / Restore

The bidder shall be responsible for backup of storage as per the policies of OCAC. These policies would be discussed with the bidder at the time of installation and configuration.

- a. The Bidder shall be responsible for monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to related retention policies
- b. The Bidder shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by OCAC or in case of upgrades and configuration changes to the system.
- c. The Bidder shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. The bidder shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.
- d. The administrators shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite).
- e. The Bidder shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre.

### 6.7.8 Network Monitoring

The Bidder shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis.

- a. The Bidder shall be responsible for monitoring and administering the network within the Data Centre up to the integration points with WAN. The bidder will be required to provide network related services for routers, switches, load balancer services etc.
- b. The Bidder shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.
- c. The Bidder would also be responsible for the overall SDN solution within the data Centre and its integration with other infrastructure orchestration solutions such as NMS, EMS and Cloud Management etc.
- d. The bidder shall co-ordinate with the Data Centre Site Preparation vendor in case of break fix maintenance of the LAN cabling or maintenance work requiring civil work.



### 6.7.9 Firewall Monitoring and Management

1. Installation and maintenance of the firewall
2. Firewall Hardening with initial configuration
3. Performance Monitoring
4. Regular Monitoring of the LAN errors
5. Firewall Rule based policy changes
6. Security Policy Configuration
7. Create and maintain Network Access Policy (NAP) document (the access specification) agreed between the parties from time to time.
8. Log File review and analysis of information on traffic flow
9. Log File trend upgrade and analysis
10. Compliance Testing
11. Design, configure and maintain all Network Address Translation (NAT) services.
12. Access control management through creation of the Network Access Policy and firewall rules
13. Implementation and maintenance.
14. Manage access to F/W logs policies and performance statistics for viewing through secure web portals in conjunction with monitoring tools
15. Manage the functioning of Regular Reports in conjunction with monitoring tools so as to provide detailed auditing of configuration history and change of journals. Alerts include critical configuration changes, potential malicious activity and operational alarms
16. Incidence response
17. Lifecycle Management of all Hardware and Software components
18. Firewall Backup.

### 6.7.10 Network Based Intrusion Prevention System - Monitoring and Management

1. Traffic Profiling
2. Define Alert levels and Incident response level
3. Root cause analysis
4. Technical support
5. Monitor NIPS for 24\*7 availability
6. Restore NIPS availability
7. Determine Intrusion occurrence
8. Upgrade of vendor provided intrusion signatures
9. Provide security event correlation
10. Regular Monitoring of the attack logging rules' logs
11. Regular Monitoring of the generic deny rules' logs
12. Regular Monitoring of the attack bandwidth utilization
13. Network attacks and serious attack attempts analysis
14. Uncovered new vulnerabilities assessment
15. Propose corrective and preventive actions.
16. Monitoring and subscribing to external network security information in order to evaluate new attacks and propose preventive steps.
17. Installation and configuration of NIPS Software and Hardware
18. Provide maintenance and upgrade of service component Software

19. Provide reporting of intrusions and actions, web based access
20. Regular Reports
21. Incidence response
22. Prevent all known network based attacks
23. Filter out IP and TCP illegal packet types
24. Design and Configuring IPS services in response to Flooding limits (per source, destination and intensity)
25. Technical Support desk Support
26. Lifecycle Management of all Hardware and Software components
27. 24\*7 Real time Monitoring and Response.

#### 6.7.11 Patch Management

The Bidder will be required to provide services related to Patch Management. The security administrators should be aware of security precautions in place in their environment.

Ensure that there is available documentation of approval as to what traffic is being allowed through to the internal network. Personnel designated to evaluate patch stability should have expertise in mission critical systems and be capable of verifying stability of systems after patch installation.

Before any patch is installed, a full backup of all data and server configuration information must be made. Best practices for disaster recovery recommend periodic testing of the restore process to ensure the integrity of the backed up data. The patch management should be executed efficiently for all kinds of environments like for operating systems and Data bases.

#### 6.7.12 Monitoring & Management

- a. The proposed service management system should provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
- b. The system should provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
- c. The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.
- d. The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service that specify the service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, quarterly and as and when required by OCAC).
- e. SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
- f. The system must provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA must be available.

### 6.7.13 Other Support Services

- a. Hardware support for the IT infrastructure solution which will include diagnosing the problem and getting the same resolved through coordination with the respective vendors as per the severity level assigned to it to ensure uptime of all IT infrastructure of OCAC as per the SLAs defined in Service Level Agreement.
- b. Maintain a record of all the hardware changes made in the IT infrastructure solution.
- c. Schedule maintenance of the IT infrastructure solution under the scope of work at the periodicity defined by the OEM and also as per the schedule defined in discussion with OCAC.
- d. Installation, upgrade, update and management of all the patches including but not limited to the servers, switches etc.
- e. Maintain the inventory of the entire hardware and software assets installed at the Data Centre.
- f. The Bidder shall maintain all documentation related to material movement such as new hardware, spare parts or equipment going out of premises for repairing etc.
- g. The Bidder shall also maintain other site specific documentation such as network diagrams, manuals, license copies in hard and soft formats.
- h. The Bidder shall also update changes to documents like changes in IP addresses, changes to layout of machines, addition to network, change in network layout, etc.
- i. The Bidder shall ensure implementation and enforcement of procedures, policies and guidelines like Security policy, Network access policy, Anti-virus policy, etc. as formulated in discussion with OCAC.
- j. The Bidder shall be responsible for Liaison with the data Centre teams for utilities such as Power, UPS, Air Conditioning, etc. as and when required.
- k. Onsite Support to ICT Infrastructure hosted by other Government Agencies: Co-location  
OCAC shall provide the Data Centre rack space to other Government agencies and user departments to host their IT Infrastructure.

The Bidder shall provide onsite support to such Government Agencies and user departments. The bidder shall be responsible for providing all the onsite support services as mentioned in this section.

## 6.8. Health Safety Environment

### **HSE Team Responsibilities:**

- Ensure all workers are knowledgeable and have access to the latest publications of applicable laws and regulations, including:
- HSE rules and safe work standards;
- Operating and critical task procedures;
- Emergency response procedures; and
- Environmental protection requirements;
- Ensure worksites offer safe and healthy working conditions;
- Ensure property and equipment are maintained to Company and manufacturer standards;
- Ensure site-specific safe work practices (e.g., start-up and shutdown practices) are developed for each facility as required, and implement training of site employees and contractors to ensure procedures are understood;
- Communicate HSE performance expectations, requirements and results to employees and contractors;
- Reinforce program objectives, policies and regulatory requirements by insisting on performance and behaviour that meet Company standards;
- Ensure compliance and incident reports are submitted as required;
- Ensure incidents are investigated and followed up with appropriate corrective actions;
- Identify training programs and opportunities as needed;
- Understand regulatory requirements;
- Understand and implement the corporate HSE Management System;
- Identify, eliminate or minimize hazards;
- Identify and correct unsafe work habits;
- Ensure workers are properly qualified and trained to perform their work, know what is expected of them, and are prepared to deal with the hazards of their work and worksites;
- Monitor work to ensure contractors and their employees comply with corporate standards and government legislation and regulation;
- Ensure personal protective equipment is available, properly used, maintained and replaced as necessary;
- Monitor facilities for HSE performance, hazards and general housekeeping standards;
- Assist management in the continued development of HSE programs;
- Ensure required pre-job meetings and regular HSE meetings are held and recorded; and
- Review inspection, audit reports, and respond to reported deficiencies.

**Employees and workers will meet the following HSE responsibilities:**



- Learn and abide by HSE standards and regulations that pertain to their work, and contact a supervisor if there is any confusion over what is required;
- Take an active part in learning, developing and promoting HSE programs and goals;
- Refuse to perform work they are not qualified to do or when unsafe conditions exist;
- Attempt to correct unsafe or hazardous conditions. Where conditions cannot be corrected, report the hazards to a supervisor;
- Immediately report all incidents to a supervisor;
- Keep written records of incidents;
- Maintain the appearance of Company facilities and promote good relations with local officials and residents;
- Maintain and operate equipment in a manner that minimizes leaks, spills, emissions, noise and other hazards;
- Know the locations of emergency, personal protective and spill response equipment and how to properly use it;
- Clean up and report spills as they occur; and Monitor activities of fellow employees and workers, especially new or inexperienced workers, to ensure they do not place themselves or others at risk.

### **Visitors**

A visitor is anyone who will be on a worksite for a short period of time (e.g., less than a day) and who must be accompanied at all times to ensure he or she is protected from the hazards on the site. Visitors include government representatives, students, senior Company employees and others. Visitors will meet the following HSE responsibilities:

1. Refrain from entering Company property or worksites except when permission has been granted by a Company supervisor, and only when accompanied by a Company representative, unless otherwise approved; and
2. Wear appropriate protective clothing and equipment in accordance with the standard requirements for the area and work conditions.

Half yearly health check must be performed each year till the end of contract period by the system integrator for Power, HVAC and other safety and monitoring systems. The system integrator may engage a third party auditor who has experience in power quality audit, HVAC audit and IBMS audit experience for Data Centres /MSCs etc. The system integrator or the third party auditing firm must use Power quality analyser ( class A), thermal imager, Air hood, Temperature loggers and other instruments for the audit and submit a comprehensive report to OCAC. All parameters such as V, I, KVA, KW, KVAR, PF, Hz, Unbalance, Harmonics (till 7th harmonics), Sags, Swells for power must be audited. For HVAC the parameters measured may be CFM, Airflow, Return and supply temperature logging for 1 hours on each PAHU/PAC, Ampere, kw, Rate of flow through ultrasonic sensor etc.



## 7. Minimum Technical Specification – IT

### 7.1. Server Type A & B – Rack Server

S/N	Minimum Requirement Specification	
1	Processor	The server should have 2 nos. of Intel Xeon latest Generation Processor: Server Type A: - 18 servers with 2 x 16 cores or higher, minimum 2.8 GHz clock rate. Server Type B: - 30 servers with 2 x 28 cores or higher, minimum 2.1 GHz clock rate. 64-bit x86 processor fully binary compatible to 32-bit applications. Number of cores on a single die/socket will be treated as a single processor
2	Memory	576 GB latest DDR memory using minimum 32 GB DIMM's and upgradable to twice asked capacity. The proposed expandability should be met by adding more memory modules of same /higher capacity. Advanced ECC with multi-bit error protection
3	HDD Controller	12 Gbps SAS RAID Controller supporting RAID 0, 1, 5 and 6 with 2GB battery backed up Cache
4	HDD	Type A - 4x 600 GB SAS Hot swap HDD (15Krpm or higher) Type B - 4 x 300 GB SAS Hot Swap HDD (15Krpm or higher)
5	Video Controller	Integrated Graphics Controller
6	Network Controller	Server Type A :- Minimum 2 x 1 Gbps ports & Two no's Dual 10/25 Gbps SFP28 (25G-SR populated) ports with four nos of 5 mtr of FC cable Server Type B:- Minimum 2 x 1 Gbps ports & Four no's Dual 10/25 Gbps SFP28 (25G-SR populated) ports with eight nos of 5 mtr of FC cable
7	Fiber Channel HBA	Two no's Dual FC Port 16 Gbps with four no's of 5mtr LC-LC Cable
8	Slots	Minimum one free PCI/PCI-x/PCI-Express
9	Ports	2* USB; 1* Keyboard Port & 1*Mouse Port (on board/dongle), One dedicated Ethernet Port for OS independent out-of-band hardware management.
10	Bays	Minimum 8 Hot Swap drive bays
11	Optical Drive	DVD ROM Internal/External
12	System Chassis	Rack Mount, 2U (max), Redundant Hot Swappable Power Supply with platinum efficiency
13	OS Certification	Certification for latest Server version of Windows and minimum two Linux flavours
14	Drive / Software Utilities	All required device drivers for OS installation, System Configuration and Server Management
15	System Management	<ul style="list-style-type: none"> <li>Monitoring ongoing management, service alerting, reporting and remote management with embedded dedicated Gigabit out of band</li> </ul>

S/N	Minimum Requirement Specification	
		<p>management port. Remote Management of Server over LAN &amp; WAN with SSL encryption, Virtual Media and virtual folder with required advanced license, Remote KVM, Server Health logging, Directory Services compliance (AD or LDAP), Multi- factor authentication, REST/XML API, group management of power, configuration, licenses including firmware, Configuration backup, Syslog (local &amp; remote).</p> <ul style="list-style-type: none"> <li>• Management software should support integration with popular virtualization platform management software like VCentre, SCVMM and Red Hat RHEV.</li> <li>• Offered Server platform must be ready for container workload deployment</li> </ul>
16	Serviceability	<ul style="list-style-type: none"> <li>• System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone support. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur. Should provide remote firmware update functionality.</li> <li>• Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD. Solution should help simplify the infrastructure management plan.</li> <li>• Solution should be provided for monitoring &amp; analysis feature to predict, prevent and auto-resolve problems and by providing automating case creation and log file submission for the problems that can't be auto-resolved. Solution shall help simplify the infrastructure management plan. Should provide silicon based hardware root of trust, automatic secure BIOS recovery, cryptographically signed firmware updates.</li> </ul>
17	Virtualization	Should support Industry Standard Virtualization Software
18	IDC Ranking	OEM should be ranked within Top 5 as per IDC report for Server in India for any quarter of 2019, Letter/Report from IDC should be attached along with the bid
19	Warranty	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support
20	IPv6 Support	All devices should be IPv6 implementation ready from day 1. No extra cost will be borne by OCAC for IPv6 implementation.
21	OEM Criteria	<p>a) Server OEM shall be in the leader's quadrant of the latest published Gartner's MQ report on Modular Servers.</p> <p>b) OEM must have India presence for last 5 years on both Sales and Support operation.</p>

## 7.2. Core Router

S/N	Minimum Requirement Specification
	<b>WAN interfaces</b>
1	The Router should support 1G,10G WAN ports
2	The Router should support internal loopback testing for maintenance purposes and an increase in availability, loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility
3	The Router should support minimum 4 payload/module slots or more
	<b>Performance</b>
4	The Router should provide minimum aggregate throughput bandwidth of 5 Gbps scalable up to 20 Gbps and 14 Mpps of forwarding performance or more.
5	The Router should have 100000 entries (IPv4), 100000 entries (IPv6) in forwarding information base or Routing table size and at least 2000 multicast routes.
	<b>Resiliency and high availability</b>
6	The Router should support Separate data and control planes to provide greater flexibility and enable continual services. Router shall offer with hardware redundant supervisor/management module
7	The Router should support Hot-swappable modules
8	The Router should have redundant hot-swappable power supply
9	The Router should support Virtual Router Redundancy Protocol (VRRP)
10	The Router should support Graceful restart including graceful restart for OSPF, IS-IS, BGP, LDP, and RSVP.
11	The Router should support nonstop forwarding (NSF) and nonstop routing
12	The Router should support Hitless software upgrades
13	The Router should support IP Fast Reroute Framework (FRR)/Multicast over FRR
	<b>Architecture</b>
14	The Router should support Distributed processing
15	The Router should support powerful processing, encryption, and comprehensive HQoS functionalities with four levels and minimum of 32K hardware queues.
16	19" rack mountable design. Must be offered with rack mounting kit.
	<b>Layer 3 routing</b>
17	The Router should support Static IPv4 routing
18	The Router should support Routing Information Protocol (RIP) V2
19	The Router should support Open Shortest Path First (OSPF) ,Interior Gateway Protocol (IGP) uses link-state protocol for faster convergence; supports ECMP and MD5 authentication for increased security and graceful restart for faster failure recovery
20	The Router should support Border Gateway Protocol 4 (BGP-4)
21	The Router should support Intermediate system to intermediate system (IS-IS) Interior Gateway Protocol (IGP) uses path vector protocol
22	The Router should support Static IPv6 routing
23	The Router should maintain separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design
25	The Router should support OSPF for IPv6

26	The Router should support BGP-4 to support Multiprotocol BGP (MBGP), including support for IPv6 addressing
27	The Router should support IS-IS for IPv6
28	The Router should support IPv6 tunneling
29	The Router should support Multiprotocol Label Switching (MPLS)
30	The Router should support Multiprotocol Label Switching (MPLS) Layer 3 VPN
31	The Router should support Multiprotocol Label Switching (MPLS) Layer 2 VPN
32	The Router should support Policy routing
33	The Router should support Multicast VPN
34	The Router should support Virtual Private LAN Service (VPLS)
35	The Router should support Bidirectional Forwarding Detection (BFD)
36	The Router should support IGMPv1, v2, and v3
37	The Router should support PIM-SSM, PIM-DM/ PIM-SM (for IPv4 and IPv6) and support IP Multicast address management and inhibition of DoS attacks
38	The Router should support Equal-Cost/Unequal-Cost Multipath (ECMP/UCMP)
39	The Router should support OSPFv3 Multi-VPN-Instance
40	The Router should support OSPFv3 Multi-VPN-Instance /6PE feature to create and maintain separate OSPFv3 routing tables for each IPv6 VPN 6PE to isolate VPN services in the device
	<b>Layer 3 services</b>
41	The Router should support Address Resolution Protocol (ARP)
42	The Router should support User Datagram Protocol (UDP) helper
43	The Router should support Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)
44	The router should support Data Centre features like DCI, EVPN, VXLAN and SDN Gateway translation functionality like VXLAN to VLAN, NVGRE to VLAN
	<b>Security</b>
45	The Router should support Dynamic Virtual Private Network (DVPN), IPSEC VPN or any equivalent mechanism or equivalent
48	The Router should have Stateful firewall
50	The Router should support powerful ACLs for both IPv4 and IPv6 to use for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; and support rule based on a Layer 2 header or a Layer 3 protocol header and specific dates or times
52	The Router should support Secure shell (SSHv2)
53	Remote Authentication Dial-In User Service (RADIUS)
54	The Router should support Terminal Access Controller Access-Control System (TACACS+)
	<b>Quality of Service (QoS)</b>
55	The Router should support HQoS/Nested QoS with four levels and minimum of 32K hardware queues
56	The Router should support Traffic policing and support Committed Access Rate (CAR) and line rate
57	The Router should support Congestion management technique like FIFO/PQ/ CQ/ WFQ/ CBQ/ RTPQ
58	The Router should support Congestion avoidance technique Weighted Random Early Detection (WRED)/Random Early Detection (RED)
59	The Router should support traffic shaping, MPLS QoS, and MP QoS/LFI

<b>Management</b>	
60	The Router should support Industry-standard CLI with a hierarchical structure
61	The Router should support SNMPv1, v2, and v3
62	provide complete support of SNMP; provide full support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption; provide alerts (via SNMP, logging, and/or SMTP) for system health and blocking/filtering actions
63	The Router should support enables or disables console port, Telnet port, or reset button interfaces depending on security preferences:
64	The Router should support Remote monitoring (RMON)
<b>Management security</b>	
65	The Router should restricts access to critical configuration commands and offers multiple privilege levels with password protection, ACLs provide Telnet and SNMP access, local and remote syslog capabilities allow logging of all access
66	The Router should support FTP, TFTP, and SFTP support
67	The Router should support ping and traceroute for both IPv4 and IPv6
68	The Router should support Network Time Protocol (NTP)
69	The Router should support RFC3164 Syslog Support
<b>Multicast support</b>	
71	The Router should support Internet Group Management Protocol (IGMP)
73	The Router should support Multicast Source Discovery Protocol (MSDP)
74	The Router should support Multicast Border Gateway Protocol (MBGP)/BGP
<b>Required Interfaces</b>	
75	4 no's 10G SFP+ ports (down gradable to 1G) and 8 no's 1G BaseT ports equally distributed across redundant slots. It has to be populated with 2x1G and 2x10G Fiber based SFP transceiver module and 8x1G copper based transceiver module from Day 1.
76	Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)
<b>OEM Criteria</b>	
77	Router OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on DCNI.
78	OEM must have India presence for last 5 years on both Sales and Support operation.
79	The router and switch should be from same OEM for ease of troubleshooting, management and data centre interconnect and overlay features like Geneve, VXLAN, EVPN has to seamlessly work across routing and switching domain.

### 7.3. Spine Switch

S/N	Minimum Requirement Specification
<b>Architecture</b>	
1	Modular architecture with 99.999% availability hardware and software design in 19" rack mountable configuration. Minimum eight slots for interface modules. Rack mounting kit must be provided.
2	Shall have two dedicated management module slots in addition to the interface modules
3	Shall have CLOS Architecture defined using Spine, Leaf and Geneve, VXLAN + ISIS or VXLAN + EVPN Protocol or equivalent shared switch fabric capability with multiple switch fabrics all supporting active switching to support high switching capacity.
4	Shall have fully distributed architecture with separation of data and control planes to deliver enhanced fault tolerance with zero service disruption during planned or unplanned events (any additional hardware required for the same shall be proposed).
5	Shall provide distributed Layer-2 (switching) and Layer-3 forwarding (Routing) /FCoE on all line cards (any additional hardware required for the same shall be proposed)
6	Shall have routing/switching capacity of minimum of 30 Tbps or more and wired speed non-blocking forwarding performance.
8	Shall support latest Ethernet technologies such as 40G, and 100G ready from day-1.
9	Shall be based on modular operating system to support enhanced serviceability along with independent process monitoring.
10	Shall deliver a maximum of 6 micro second or less latency with consistent performance across a broad range of applications with typical mixed loads of real-time and multicast traffic.
<b>Data Centre Features (any additional licenses required shall be included)</b>	
11	Shall have data Centre virtualization capability that enables multi-tenancy into multiple logical devices (with each logical switch having its own tenants where each logical switch has its own processes, configuration, and administration). or VXLAN
12	Shall provide Geneve, VxLAN feature for both L2 and L3
13	Shall support In Service Software Upgrade (ISSU) or hit less update or equivalent architecture to provide an upgrade of the entire chassis or an individual task/process without impacting hardware forwarding.
14	Shall have Data Centre Bridging (DCB) protocols such as IEEE 802.1Qaz Data Centre Bridging Exchange (DCBX), Enhanced Transmission Selection (ETS), and IEEE 802.1Qbb Priority Flow Control (PFC) features in all offered ports
15	Shall support Large Layer 2 scaling through advanced features such as Transparent Interconnection of Lots of Links (TRILL) or equivalent feature, 90K MAC entries or higher per each offered interface module.
<b>Resiliency</b>	
16	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to aggregate the links
17	Shall have Redundant switch fabrics (N+1), Redundant management modules (1+1), power supplies (N+1), and fan trays/fans (1+1) from Day 1.



S/N	Minimum Requirement Specification
18	Passive backplane with no active components for increased system reliability
19	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
20	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
21	Virtual Router Redundancy Protocol (VRRP) to allow a group of switches to dynamically back each other up to create highly available routed environments
22	Graceful restart for OSPF, IS-IS and BGP protocols
23	Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS, VRRP and BGP protocols
<b>Layer 2 Features</b>	
24	Shall support up to 16 Nos. of link or more per Port channel (using LACP)
25	Spanning Tree Protocol (IEEE 802.1D, 80802.1W, 80802.1S)
26	Shall support Jumbo frames of 9K bytes
27	Internet Group Management Protocol (IGMP)
28	Shall support for broadcast, multicast and unknown unicast storm control
29	Multicast Listener Discovery (MLD) or IGMP snooping
30	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
31	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
<b>Layer 3 Features (any additional licenses required shall be included)</b>	
32	Static Routing, RIP, OSPF, IS-IS, BGP for IPv4 and IPv6
33	Policy-based routing, ECMP, 32K Routing entries per each offered interface module.
34	Dynamic Host Configuration Protocol (DHCP) /Client/ Relay / server
35	Sparse Mode (PIM-SM)/ Source-Specific Mode (PIM-SSM) for IPv4 and IPv6 multicast applications
<b>QoS and Security Features</b>	
36	Shall have access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network
37	Shall support Port-based rate limiting and access control list (ACL) based rate limiting
38	Shall have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle -attack, Replay Attack, Data Disclosure, Denial of Service
39	Shall create traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence
40	Shall support Strict Priority Queuing (SP)/ Weighted Fair Queuing (WFQ)/ Weighted Deficit Round Robin (WDRR), configurable buffers and Explicit Congestion Notification (ECN)
41	Shall support VM attribute based zoning and policy and support Micro Segmentation for the Virtualize and Non – Virtualize environment
42	Switch should support securing the access to an access or trunk port based on MAC address.
43	Shall be accessible using CLI over SSH and GUI using HTTP/HTTPS
44	Switch should support MAC Address Notification, DHCP Snooping
45	Shall support Weighted Random Early Detection (WRED) / Random Early Detection (RED) for congestion avoidance
46	DHCP protection/snooping to block DHCP packets from unauthorized DHCP servers
47	ARP attack protection to protect against attacks that use a large number of ARP requests

S/N	Minimum Requirement Specification
48	Shall support Packet storm protection to protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds
<b>Management Features</b>	
49	Configuration through the CLI, console, Telnet, and SSH
50	SNMPv1, v2, and v3 and Remote monitoring (RMON) support
51	NetFlow/ sFlow or equivalent for traffic analysis
52	Should support tools like Ping and Traceroute
53	Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port.
54	RADIUS/TACACS+ for switch security access administration
55	Network Time Protocol (NTP) or equivalent support
<b>Required Interfaces</b>	
56	Minimum 64 ports of 40G/100G and 2 Ports of 100G QSFP+ equally distributed across interface modules
57	Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)
58	Minimum 2 interface modules must be free for future use after meeting the requirement as above.
<b>OEM Criteria</b>	
59	Switch OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on DCNI.
60	OEM must have India presence for last 5 years on both Sales and Support operation.

#### 7.4. Leaf Switch (Fibre)

S/N	Minimum Requirement Specification
<b>Architecture</b>	
1	19" rack mountable configuration. Rack mounting kit must be provided.
2	Shall have fully distributed architecture with separation of data and control planes to deliver enhanced fault tolerance with zero service disruption during planned or unplanned events (any additional hardware required for the same shall be proposed).
3	Shall provide distributed Layer-2 (switching) and Layer-3 forwarding (Routing) on all offered ports (any additional hardware required for the same shall be proposed)
4	Shall have routing/switching capacity of minimum of 2.66 Tbps or more, speed non-blocking forwarding performance.
5	Shall support latest Ethernet technologies such as 10G, 25G, 40G, and 100G ready from day-1
6	Shall be based on modular operating system to support enhanced serviceability along with independent process monitoring.
7	Shall deliver a maximum of 6ms latency with consistent performance across a broad range of applications with typical mixed loads of real-time, multicast and storage traffic.
<b>Data Centre Features (any additional licenses required shall be included)</b>	
8	Shall provide VxLAN feature for L2 orL3

9	Shall support In Service Software Upgrade (ISSU) or hit less update to provide an upgrade of the entire chassis or an individual task/process without impacting hardware forwarding
10	Shall have Data Centre Bridging (DCB) protocols such as IEEE 802.1Qaz Data Centre Bridging Exchange (DCBX), Enhanced Transmission Selection (ETS), and IEEE 802.1Qbb Priority Flow Control (PFC) along with Fibre Channel over Ethernet (FCoE) features in all offered ports
11	Shall support Large Layer 2 scaling through advanced features such as Transparent Interconnection of Lots of Links (TRILL) or equivalent feature, 90K MAC entries
	<b>Resiliency</b>
12	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to aggregate the links
13	Shall have redundant power supplies (1+1), and fan/fan trays (N+1) from Day 1.
14	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
15	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
16	Virtual Router Redundancy Protocol (VRRP) to allow a group of switches to dynamically back each other up to create highly available routed environments
17	Graceful restart for OSPF, IS-IS and BGP protocols
18	Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS, VRRP and BGP protocols
	<b>Layer 2 Features</b>
19	Shall support up to 3950 Vlan or IEEE 802.1Q-based VLANs
20	Shall support Jumbo frames of 9K bytes
21	Internet Group Management Protocol (IGMP)
22	Multicast Listener Discovery (MLD)/IGMP snooping
23	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
24	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	<b>Layer 3 Features (any additional licenses required shall be included)</b>
25	Static Routing, RIP, OSPF, IS-IS, BGP for IPv4 and IPv6
26	Policy-based routing, ECMP, 64K Routing entries
27	Dynamic Host Configuration Protocol (DHCP) client/ Relay and server
28	Sparse Mode (PIM-SM)/ Source-Specific Mode (PIM-SSM) for IPv4 and IPv6 multicast applications
	<b>QoS and Security Features</b>
29	Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network
30	Port-based rate limiting and access control list (ACL) based rate limiting
31	Shall create traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence
32	Shall support Strict Priority Queuing (SP), Weighted Fair Queuing (WFQ)/Weighted Deficit Round Robin (WDRR)/ configurable buffers and Explicit Congestion Notification (ECN)
33	Shall support Random Early Detection (RED) for congestion avoidance
34	DHCP protection/snooping to block DHCP packets from unauthorized DHCP servers
35	ARP attack protection to protect against attacks that use a large number of ARP requests

36	Port security to allow access only to specified MAC addresses
37	Shall support Packet storm protection to protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds
	<b>Management Features</b>
38	Configuration through the CLI, console, Telnet, and SSH
39	SNMPv1, v2, and v3 and Remote monitoring (RMON) support
40	NetFlow/sFlow or equivalent for traffic analysis
41	Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port.
42	RADIUS/TACACS+ for switch security access administration
43	Network Time Protocol (NTP) or equivalent support
	<b>Required Interfaces</b>
44	48 ports of 10/25G SFP+ and 4 ports of 40G QSFP+ per Interface module
45	Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)
	<b>OEM Criteria</b>
46	Switch OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on DCNI.
47	OEM must have India presence for last 5 years on both Sales and Support operation.

### 7.5. Leaf Switch (Copper)

S/N	Minimum Requirement Specification
	<b>Architecture</b>
1	19" rack mountable configuration. Rack mounting kit must be provided.
2	Shall have fully distributed architecture with separation of data and control planes to deliver enhanced fault tolerance with zero service disruption during planned or unplanned events (any additional hardware required for the same shall be proposed).
3	Shall provide distributed Layer-2 (switching) and Layer-3 forwarding (Routing) on all offered ports (any additional hardware required for the same shall be proposed)
4	Shall have routing/switching capacity minimum of 1.25 Tbps of forwarding performance
5	Shall support latest Ethernet technologies such as 10G, 40G from day-1 while remaining backward compatible to 1G.
6	Shall be based on modular operating system to support enhanced serviceability along with independent process monitoring.
7	Shall deliver a maximum of 6micro second latency with consistent performance across a broad range of applications with typical mixed loads of real-time, multicast and storage traffic.
	<b>Data Centre Features (any additional licenses required shall be included)</b>
8	Shall provide VxLAN feature for L2/L3

S/N	Minimum Requirement Specification
9	Shall support In Service Software Upgrade (ISSU) or hit less update to provide an upgrade of the entire chassis or an individual task/process without impacting hardware forwarding
10	Shall have Data Centre Bridging (DCB) protocols such as IEEE 802.1Qaz Data Centre Bridging Exchange (DCBX), Enhanced Transmission Selection (ETS), and IEEE 802.1Qbb Priority Flow Control (PFC) along with Fibre Channel over Ethernet (FCoE) features in all offered ports
11	Shall support Large Layer 2 scaling through advanced features such as TRansparent Interconnection of Lots of Links (TRILL) or equivalent feature, 90K MAC entries
	<b>Resiliency</b>
12	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to aggregate the links
13	Shall have redundant power supplies (1+1), and fan/fan trays (1+1) from Day 1.
14	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
15	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
16	Virtual Router Redundancy Protocol (VRRP) to allow a group of switches to dynamically back each other up to create highly available routed environments
17	Graceful restart for OSPF, IS-IS and BGP protocols
18	Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS, VRRP and BGP protocols
	<b>Layer 2 Features</b>
19	Shall support up to 3950 vlan or IEEE 802.1Q-based VLANs
20	Shall support Jumbo frames of 9K bytes
21	Internet Group Management Protocol (IGMP)
22	Multicast Listener Discovery (MLD) or IGMP Snooping
23	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
24	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	<b>Layer 3 Features (any additional licenses required shall be included)</b>
25	Static Routing, RIP, OSPF, IS-IS, BGP for IPv4 and IPv6
26	Policy-based routing, ECMP, 32K Routing entries
29	Dynamic Host Configuration Protocol (DHCP) client/Relay and server
30	Sparse Mode (PIM-SM)/ Source-Specific Mode (PIM-SSM) for IPv4 and IPv6 multicast applications
	<b>QoS and Security Features</b>
31	Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network
32	Port-based rate limiting and access control list (ACL) based rate limiting
33	Shall create traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence
34	Shall support Strict Priority Queuing (SP), Weighted Fair Queuing (WFQ)/Weighted Deficit Round Robin (WDRR)/configurable buffers and Explicit Congestion Notification (ECN)
35	Shall support Random Early Detection (RED) for congestion avoidance
36	DHCP protection/snooping to block DHCP packets from unauthorized DHCP servers

S/N	Minimum Requirement Specification
37	ARP attack protection to protect against attacks that use a large number of ARP requests
38	Port security to allow access only to specified MAC addresses
39	Shall support Packet storm protection to protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds
	<b>Management Features</b>
40	Configuration through the CLI, console, Telnet, and SSH
41	SNMPv1, v2, and v3 and Remote monitoring (RMON) support
42	NetFlow/sFlow or equivalent for traffic analysis
43	Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port.
44	RADIUS/TACACS+ for switch security access administration
	<b>Required Interfaces</b>
45	24 ports of 1G/10G BaseT, 24 ports of 10G SFP and 4 ports of 40G QSFP+
46	Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)
	<b>OEM Criteria</b>
47	Switch OEM shall be in the leader's quadrant as per the latest published Gartner's MQ report on DCNI.
48	OEM must have India presence for last 5 years on both Sales and Support operation.

## 7.6. Management Switch -1

S/N	Minimum Requirement Specification
	<b>Architecture</b>
1	19" rack mountable configuration. Rack mounting kit must be provided.
2	Shall have routing/switching capacity minimum of 560 Gbps and up to 389 Mpps of forwarding performance
3	Shall be based on modular operating system to support enhanced serviceability along with independent process monitoring.
4	Shall deliver a maximum of 6micro second latency with consistent performance across a broad range of applications with typical mixed loads of real-time, multicast and storage traffic.
5	32K MAC entries or more
	<b>Resiliency</b>
6	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to aggregate the links
7	Shall have redundant hot swap power supplies (1+1) from Day 1.
8	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
9	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	<b>Layer 2 Features</b>
10	Shall support up to 3950 port or IEEE 802.1Q-based VLANs
11	Shall support Jumbo frames of 9K bytes
12	Internet Group Management Protocol (IGMP)
13	Multicast Listener Discovery (MLD) or IGMP snooping
14	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
15	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	<b>Layer 3 Features (any additional licenses required shall be included)</b>
16	Static Routing for IPv4 and IPv6
17	Dynamic Host Configuration Protocol (DHCP) client/ Relay and server
	<b>QoS and Security Features</b>
18	Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network
19	Port-based rate limiting and access control list (ACL) based rate limiting
20	Shall create traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence
21	Shall support Strict Priority Queuing (SP)/Weighted Fair Queuing (WFQ)/Weighted Deficit Round Robin (WDRR)configurable buffers and Explicit Congestion Notification (ECN)
22	Shall support Weighted Random Early Detection (RED) /Random Early Detection (RED) for congestion avoidance
23	DHCP protection/snooping to block DHCP packets from unauthorized DHCP servers
24	ARP attack protection to protect against attacks that use a large number of ARP requests
25	Port security to allow access only to specified MAC addresses

S/N	Minimum Requirement Specification
26	Shall support Packet storm protection to protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds
	<b>Management Features</b>
27	Configuration through the CLI, console, Telnet, and SSH
28	SNMPv1, v2, and v3 and Remote monitoring (RMON) support
29	NetFlow/sFlow or equivalent for traffic analysis
30	Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port.
31	RADIUS/TACACS+ for switch security access administration
32	Network Time Protocol (NTP) or equivalent support
	<b>Required Interfaces</b>
33	24 ports of 1G/10G BaseT and 4 ports of 10G SFP+
35	Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)
	<b>OEM Criteria</b>
36	Switch OEM shall be in the leader's quadrant as per latest published Gartner's MQ report on DCNI or Wired & Wireless LAN Access Infrastructure.
37	OEM must have India presence for last 5 years on both Sales and Support operation.

### 7.7. Management Switch -2

S/N	Minimum Requirement Specification
	<b>Architecture</b>
1	19" rack mountable configuration. Rack mounting kit must be provided.
2	Shall have routing/switching capacity of minimum of 1 Tbps or more and up to 1520 Mpps of forwarding performance.
3	Shall be based on modular operating system to support enhanced serviceability along with independent process monitoring.
4	Shall deliver a maximum of 6 Micro Second latency with consistent performance across a broad range of applications with typical mixed loads of real-time, multicast traffic.
5	32K or more MAC entries
	<b>Resiliency</b>
6	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to aggregate the links.
7	Shall have redundant hot swap power supplies (1+1) from Day 1.
8	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
9	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	<b>Layer 2 Features</b>
10	Shall support up to 3950 port or IEEE 802.1Q-based VLANs
11	Shall support Jumbo frames of 9K bytes
12	Internet Group Management Protocol (IGMP)
13	Multicast Listener Discovery (MLD)/IGMP snooping



S/N	Minimum Requirement Specification
14	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
15	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
<b>Layer 3 Features (any additional licenses required shall be included)</b>	
16	Static Routing for IPv4 and IPv6
17	Dynamic Host Configuration Protocol (DHCP) Client/ Relay / server
<b>QoS and Security Features</b>	
18	Access Control Lists for both IPv4 and IPv6 for filtering traffic to prevent unauthorized users from accessing the network
19	Port-based rate limiting and access control list (ACL) based rate limiting
20	Shall create traffic classes based on access control lists (ACLs), IEEE 802.1p precedence, IP, and DSCP or Type of Service (ToS) precedence
21	Shall support Strict Priority Queuing (SP)/ Weighted Fair Queuing (WFQ)/ Weighted Deficit Round Robin (WDRR), configurable buffers and Explicit Congestion Notification (ECN)
22	Shall support Weighted Random Early Detection (WRED)/RED for congestion avoidance
23	DHCP protection/snooping to block DHCP packets from unauthorized DHCP servers
24	ARP attack protection to protect against attacks that use a large number of ARP requests
25	Shall support Packet storm protection to protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds
<b>Management Features</b>	
26	Configuration through the CLI, console, Telnet, and SSH
27	SNMPv1, v2, and v3 and Remote monitoring (RMON) support
28	NetFlow/sFlow or equivalent for traffic analysis
29	Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port.
30	RADIUS/TACACS+ for switch security access administration
31	Network Time Protocol (NTP) or equivalent support
<b>Required Interfaces</b>	
32	48 ports of 1G/10G BaseT and 4 ports of 10G SFP+
33	Transceiver modules shall be suitable for MMF cabling inside the DC (preferably with LC interface)
<b>OEM Criteria</b>	
34	Switch OEM shall be in the leader's quadrant of latest published Gartner's MQ report on DCNI or Wired & Wireless LAN Access Infrastructure.
35	OEM must have India presence for last 5 years on both Sales and Support operation.

## 7.8. San Switch (128 Ports)

S/N	Minimum Requirement Specification
1	The enterprise class fibre switch should be quoted with minimum 128 FC ports of 16Gbps speed each with necessary Licenses.
2	The switch should have non -blocking architecture.
3	The Core Fabric switch must provide 16Gbps line-rate ports per module with no oversubscription for intra-module or inter-module switching.
4	The switch should have support for 8/16 Gbps HBAs
5	The aggregate backplane bandwidth of switch should be scalable more than 4 Tbps
6	The switch should have integrated / External FCIP module. If storage array support FCIP the same can be used.
7	The switch should have No Single Point of Failure (SPOF) and all the components should be hot swappable without even scheduled down time.
8	The switch should have hot swappable N+1 redundant Power Supplies
9	The switch should have hot swappable N+1 redundant Cooling Fans
10	The switch should have feature for Non-disruptive firmware update
11	The switch should have Real time performance monitoring reporting tool
12	The switch should have support for POST & online diagnostics
13	The switch should have capability to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating Systems
14	The switch should have support of all leading SAN / NAS disk arrays and tape libraries
15	The switch should have following security features:
	Must have hardware & Software zoning
	Policy based security and centralized fabric management
	Encryption
	FC authentication
	RADIUS, SSH, SNMP port binding and Masking
16	The switch should have Inter Switch linking feature to connect two or more FC switches
17	The switch should have trunking capability. The required software license should be supplied with switch.
18	Switch should Provide Adaptive Networking services such as Quality of Service (QoS)
19	The switch should have high availability feature with no performance degradation of switching operation even when one of the processor card fails.
<b>OEM Criteria</b>	
20	OEM shall be in the leader's quadrant as per latest Gartner's MQ report for General Purpose Array OR DCNI MQ report.
21	OEM must have India presence for last 5 years on both Sales and Support operation.

## 7.9. San Switch (48 Ports)

S/N	Minimum Requirement Specification
1	The fibre switch should be quoted with minimum 48 FC ports of 16Gbps speed each with necessary Licenses.
2	The switch should have support for 8/16 Gbps HBA
3	The switch should have auto sensing, Zoning, Ethernet and Serial Port for communication.
4	Switch should be rack mountable 1U size and should be supplied with mounting kit.
5	The switch should be equipped with redundant hot swap power supply and Fan and allow hot swap ability without resetting the switch, or affecting the operations of the switch
6	The switch should be backward compatible
7	The switch should be capable for Non-disruptive firmware update.
8	The switch should be capable of End to end performance monitoring
9	The switch should have Support for POST & online diagnostics
10	The switch should be capable to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating Systems
11	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), Port Zoning and LUN Zoning
12	The switch should support IPv6 from day one.
13	Switch must support out-band management protocols like SNMPv3, SMI-S, Telnet, FTP and TFTP.
14	The switch should have following Zoning and security features:
	a. Support for hardware -enforced zoning.
	b. Policy based security and centralized fabric management.
	c. Support for secure access.
	d. Support for FC based authentication.
	e. Support for TACACS+ or RADIUS, SSH, SNMP
	f. Support for port binding.
	g. Support for port masking.
	h. Support for Hardware based Inter Switch linking / trunking.
i. Support for dynamic Load balancing of links with no overhead.	
15	All relevant licenses for above features should be quoted along with switch
<b>OEM Criteria</b>	
16	OEM shall be in the leader's quadrant as per latest Gartner's MQ report for General Purpose Array OR DCNI MQ report.
17	OEM must have India presence for last 5years on both Sales and Support operation.

## 7.10. Enterprise Storage

S/N	Minimum Requirement Specification
1	The proposed storage system should be of Enterprise class storage. Controllers/Directors shall be true symmetrical active-active, offering scale up & scale-out architecture. Processor, global cache, disk, ports should be scaled linearly by adding multiple controllers/directors.
2	The Storage system should be Enterprise Class Storage System and supplied with 1PB usable capacity of all SSD/ Flash /FMD.
3	The enterprise storage array must be proposed with a minimum of Four controllers/directors & should be scalable up to eight controllers/directors as a single array (serial number/asset). Volume should be accessible through all controllers directly and should be striped across all disks behind all controllers/directors in the storage system at all times. If any of the controller fails the remaining controllers should manage and operate the entire storage volume. System should provide automatic load balancing ensuring that the array resources are evenly utilized without any manual intervention. The proposed enterprise class storage should also support file services natively.
4	The storage system should support non-disruptive component repair and hot replacement of Interfaces, backplane, Disk Controllers, Disk Drives, Cache memory cards, Power Supplies & Battery systems, Fan subsystems, Micro-code. The proposed storage must support non-disruptive replacement of hardware component. Architecture shall support isolation of failed components automatically without rebooting/failing the entire controller and shall support sub-controller fault isolation. The proposed storage array must be configured with NSPOF (No-single-point-of-failure) architecture.
5	The proposed storage system should support more than 20000 LUNs /Volumes
6	The storage system should support Clusters of MS-SQL, My SQL, PostgreSQL, and Windows and Linux server clusters. It should also support all enterprise level virtualization (Hyper-V, VMware, KVM, RHEL, Openstack etc.).
8	Offered storage system should have a minimum aggregate 1TB DRAM Global Cache extendible to 2TB DRAM Protected Cache, with an ability to protect data on cache if there is a controller failure or power outage. SSDs will not be considered as cache memory.
10	The cache on the storage should have minimum 48 hrs or more battery backup or should have de-staging capability to either flash/disk. (Cache of 2TB means sum of the Cache memory supported by all the Storage Controllers in the Storage. DRAM without protection against power failure like destaging/battery backup & SSD/PCIe based Flash will not be considered as Cache.)
11	The storage should be supplied with iSCSI, NFS, CIFS, FC protocols for use with different applications. All protocol licenses should be provided for entire capacity of the storage. Any hardware/software required for this functionality shall be supplied along with the storage.

12	System should have open stack cinder driver. Storage should support VMware Vstorage APIs for array integration including but not limited to VAAI, VASA, etc., ODX for Microsoft Hyper-V, and RHEL.
13	Should support various RAID levels like Single Parity RAID/ Dual Parity RAID. The Storage should support RAID 5, RAID 6, RAID10 OR Equivalent RAID Levels
14	The architecture should be designed as a NSPOF architecture. Proposed Storage must be supplied with Data-at-Rest Encryption, drive based encryption shall not be accepted and should be FIPS 140-2 compliant.
15	Proposed storage should support both block and File level Data Reduction methods, otherwise extra usable storage capacity needs to be factored.
16	The storage should be supplied with OEM rack. The storage system should be supplied with all the necessary SFP+ modules & patch cords as required.
17	The storage array shall have the ability to expand LUNS/Volumes on the storage online and instantly. The storage should support dynamic LUN/ File System expansion natively or through LVM.
18	The Storage array must provide capability for thin provisioning of capacity. This storage system will be deployed with thin provisioning, Vendor should provide the licenses for maximum supported capacity of the proposed storage. Vendor should suggest mechanism for thin reclaim from deleted space without any / minimal performance impact. Required additional hardware and Software infrastructure for thin reclaim to be quoted.
19	The storage should have granular quality of service (QoS) that allows users to assign minimum thresholds for IOPS, bandwidth and latency.
21	The proposed storage system should support zero data loss Three Way DR solution. The storage should have capability of 3 way replication with zero data loss (Synchronous to Near-DR and Asynchronous to DR i.e. 2 distinct storage arrays at DC & Near-DR ) The proposed storage solution must support both Synchronous and Asynchronous Data replication. Storage replication should be able to switch mode between Sync and Async whenever required automatic.
22	The array should support controller-based functionality for pointer based snapshot. The storage should support minimum 250 snapshots per volume/LUN. Vendor should provide the licenses for maximum supported capacity of the proposed storage. The storage should support incremental updates to minimum of 3 targets LUN's (clones) post the initial full sync simultaneously and at same time; in case storage array requires additional space reservation for Snap/Clones, the Vendor has to provision additional 20% usable capacity using the same drive capacity and RAID Levels for optimal performance.
24	Easy to use GUI based and web enabled administration interface for configuration
25	Friendly GUI Based Storage Administration tools for role based access control, monitoring, event management and closure, threshold setting, LUN mapping, deallocation, space reclaim etc.
26	GUI Based Storage Monitoring tools to obtain Storage performance statistics like Total IOPs performance, Read/write percentages, Store historical data, Management Dashboard etc.

27	The storage shall support multi-tenant environments requiring isolation of workload or dedicated physical drives through separation of resource pools / partitioning etc. Vendor should provide the licenses for maximum supported capacity of the proposed storage.
28	The proposed storage should support industry-leading Operating System platforms including: SuSE and Red Hat LINUX, Microsoft Windows, HPE-UX, SUN Solaris, IBM-AIX, etc. It shall support connecting hosts over iSCSI or FC and shall be supplied with any Multi-pathing/Equivalent software.
29	Storage subsystem shall be supplied with Thin Provisioning, Snapshot, Clone, Performance Monitoring, Quality of services, and File services on day 1 for the maximum supported capacity of array. All the licenses on the storage system must be provided for maximum capacity. Supplied with the system from day one.
30	The storage should be supplied with usable capacity of 1.0 Peta Byte from day 1 occupied with adequate controller to support usable capacity of storage up to 3 Peta Byte (Excluding any RAID overhead, Hot spare, Controller OS overhead etc.) in RAID 6. One Global spare should be provided for every 30 Drives.
31	Offered Storage array shall support integration with leading container technologies such as Docker, Open Shift, Kubernetes and MESOS etc. Vendor shall provide documentary proof for integration.
32	The designed IOPs for 30:70 Write: Read for the above systems for RAID 6 should be minimum 1million IOPS with 8K block size from SSD tier. The design document should be shared in the proposal.
33	Front-End Ports: 64 no's 16Gb FC ports, 4 no's 10Gb SFP+ ports for iSCSI, and 4 no's 10Gb ports for replication.
34	Back-End ports –Minimum 384 Gbps of aggregate bandwidth for disk drive connectivity scalable to 768Gbps across all controllers.
35	The supported disks should be dual ported with minimum 12Gbps or higher full-duplex data transfer capability.
36	The proposed storage array must be supplied with a CLI and GUI based storage management tool for the storage array. Should have capability to manage both local and remote systems from a single console and should be capable of generating alerts.
37	The storage system should be supplied mentioned licenses from day -1
<b>OEM Criteria</b>	
38	OEM shall be in the leader's quadrant as per latest Gartner's MQ report for General Purpose Disk Array.
39	OEM must have India presence for last 5 years on both Sales and Support operation.
40	OEM must be in the top 5 vendors list as per IDC report in India on external storage system by market share (by vendor revenue) for last 2 years.

## 7.11. Tape Library

S/N	Minimum Requirement Specification	
1	Capacity	<p>a) Shall support Native data capacity of more than 3PB (uncompressed) expandable to more than 4 PB (2.5:1 compressed) when fully populated, using LTO-8 or higher Technology.</p> <p>b) Shall be offered with Minimum of 15 no's LTO-8 FC tape drives.</p> <p>c) Tape Drive shall support encryption.</p> <p>d) Shall be offered with minimum 125 Cartridge slots.</p>
2	Tape Drive Architecture	Offered LTO-8 drive in the Library shall conform to the Data rate matching technique for higher reliability. Tape Drive Architecture in the Library shall conform to the INCITS/T10 SCSI-3 standard or newer standards.
3	Speed	Offered LTO-8 drive shall support 300MB/sec in Native mode.
4	Scalability	Tape Library shall be scalable to more than <b>250</b> slots and 20 number of LTO-8 Drives within the same Library.
5	Connectivity	Offered Tape Library shall provide 8Gbps native FC connectivity to SAN switches.
6	Partitioning	Offered Tape Library shall have partitioning support so that each drive can be configured in a separate partition. Offered Tape Library shall have support for at-least 20 partition.
7	Management	Tape Library shall provide web based remote management.
8	Encryption device	Offered Library shall be provided with a hardware device like USB key, separate appliance etc. to keep all the encrypted keys in a redundant fashion.
9	Barcode Reader and Mail slots	Out of 250 slots, Tape library shall support Barcode reader and at-least 10 mail slots and shall be scalable to 20 mail slots when fully populated.
10	Other Features	<p>a) Tape Library shall have GUI Panel.</p> <p>b) Shall be rack mountable and shall be offered with mounting kit.</p> <p>c) Shall have option for redundant power supply.</p> <p>d) Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action.</p> <p>e) Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved.</p>
11	OEM Criteria	<p>a) OEM shall be in the leader's quadrant as per the latest Gartner's MQ report for General Purpose Disk Array OR MQ report for DCN.</p> <p>b) OEM must have India presence for last 5 years on both Sales and Support operation.</p>

## 7.12. Link Load Balancer

S/N	Minimum Requirement Specification
1	Link Load Balancer should be dedicated appliance based solution with high performance purpose built (not a part of UTM or Firewall)
2	The appliance should have minimum 4 x 10Gb SFP+ ports (down gradable to 1G) and 4x1GE ports
3	The appliance should have 10 Gbps throughput from day one
4	The appliance should support 25 M connections
5	Support for multiple internet links in Active-Active load balancing and active-standby failover mode.
6	Should support the following Global Load balancing algorithms: <ul style="list-style-type: none"> <li>• Round robin</li> <li>• Global availability <ul style="list-style-type: none"> <li>• LDNS persistence</li> <li>• Application availability</li> <li>• Geography</li> <li>• Virtual server capacity</li> <li>• Least connections</li> <li>• Packets per second</li> <li>• Round trip time</li> </ul> </li> </ul> Additional Algorithms(optional) <ul style="list-style-type: none"> <li>• Hops</li> <li>• Packet completion rate</li> <li>• User-defined QoS</li> <li>• Dynamic ratio</li> <li>• LDNS</li> <li>• Ratio</li> </ul>
7	IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support.
8	In case of link failure, device should detect it in less than 30 seconds and divert the traffic to other available links.
9	Should provide mechanism to bind multiple health checks, support for Application specific VIP health check and next gateway health checks.
10	Should support Geolocation and Proximity based load balancing
11	Record type supported by Link Load Balancer - (A and AAAA)
12	Should support 1) Delegated DNS and 2) Proxy DNS
13	The Solution should be able to function as full-feature authoritative name server
14	Should provide comprehensive and reliable support for high availability based on Per VIP based Active-active & active standby unit redundancy mode.
	<b>OEM Criteria</b>
15	OEM should be present in Gartner's Leaders Quadrant for ADC in the latest published report or top four in the latest published IDC report.



## 7.13. Next Generation Firewall

S/N	Minimum Requirement Specification
1	The proposed solution/appliance MUST be for Layer 7 protection. There should be no performance degradation in the overall transaction processing. The solution MUST be deployed in HA mode.
2	The proposed solution must allow policy rule creation for application identification, user identification, host profile, threat prevention, content filtering, QOS and scheduling.
3	The proposed solution must allow policy creation for application identification, user identification, threat prevention and content filtering in a single window and not multiple locations
4	The proposed solution should have the features of stateful firewall, IPS, Application control, Content Inspection, Identity Inspection, Anti-BOT, Antivirus and Zero-day malware protection from day one. Proposed solution should provide a threat prevention throughput of 10 Gbps for traffic conditions enabling application visibility control, user identity, NGIPS, Antivirus and all other security threat prevention features enabled with HTTP transactions, HTTPS and traffic mix such as HTTPS, SMTP and other protocols.
5	The proposed solution should have dual redundant power supply and at least 64 GB of memory scalable up to 128 GB in order to achieve higher number of concurrent connections
6	The proposed firewall appliance should have at least 8 ports of 1 Gbps Ethernet Ports and 4 ports of 10 G SFP+ fibre ports and should support 40 G QSFP interfaces for future expansion.
7	The proposed solution must be able to support Network attack detection, DoS, DDoS, TCP Reassembly , Brute Force, Syn Cookie, IP Spoofing, Malformed Packet etc.
8	The proposed solution must support Tap mode interface configuration.
9	The proposed solution must support Transparent, Layer 2 and Layer 3 mode providing flexible deployment.
10	The proposed solution be able to support simultaneous deployment with interfaces servicing Layer 3, Layer 2 Transparent and Tap modes.
11	The proposed solution shall support 802.1Q VLAN tagging.
12	The proposed solution shall support Dual Stack IPv4 / IPv6 application control and threat inspection under various deployment modes.
13	The proposed solution shall support standards based Link aggregation (IEEE 802.3ad) to achieve higher bandwidth.
14	The proposed solution shall support logical Ethernet sub-interfaces tagged or untagged.
15	The proposed solution must support the following routing protocols static, RIPV2, OSPF and BGP4.
16	The proposed solution must have IPv6 Static Routing Support even for virtual routers.
17	The proposed solution must support Policy Based forwarding based on Zone, Applications, Source / Destination Address, User or User Group. There should not be any limit of policies to be configured.
18	The proposed solution shall support DNS proxy

S/N	Minimum Requirement Specification
19	The proposed solution shall support DHCPv4 and DHCPv6 relay
20	High Availability
21	The proposed solution must be able to support Active/Active , Active/Passive configuration
22	The proposed solution must be capable to detect device, link and path failure.
23	The proposed solution must be able to support session and configuration synchronization. Proposed appliance must support at least 4 million concurrent sessions and should be scalable to support 2 times in future and 150,000 new connections per second from day one and should be scalable to support 2 times in future. The solution should be scalable to support 25 million concurrent sessions with higher memory
24	The solution must support stateful failover
25	The proposed solution HA shall support hitless upgrades for both major and minor code releases
26	The proposed solution shall control parameters by Security Zone, Users, IP, Application, Host Information Profile, URL Category ,Schedule, QoS etc.
27	This solution should support SSL & SSH traffic decryption & inspection
28	The proposed solution shall support the following policy types/capabilities:
29	The solution must support at least 5000 applications in the application visibility database. Higher number of supported applications are preferable.
30	Policy-based control by application function (posting, file transfer, desktop sharing, instant messaging, etc.)
31	Policy-based control by user, group or IP address
32	-The solution should be able to emulate files by type: bat, cab, dll, exe, pif, reg, vbs, tar, scr, swf and tgz
33	-Data filtering: Custom Data Patterns
34	-QoS Policy-based traffic shaping (priority, guaranteed, maximum)
35	-Policy support for scheduled time of day enablement
36	The proposed solution shall have application and application function identification and decoding technology without any additional licensing policy
37	The proposed solution shall be able to handle applications with multiple action options e.g. alert, block or allow
38	The proposed solution shall be able to create custom application signatures and categories
39	The proposed solution shall allow updating the application database automatically or manually via the control or traffic plane
40	The proposed solution shall delineate specific instances of peer2peer traffic (e.g. Bit torrent, emule, neonet, etc.)
41	The proposed solution shall delineate specific instances of instant messaging (e.g. Gtalk, YIM, Facebook Chat, etc.)

S/N	Minimum Requirement Specification
42	The proposed solution shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability
43	The proposed solution shall delineate specific instances of Proxies (e.g. ultrasurf, ghostsurf, freegate, etc.)
44	The proposed solution shall support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)
45	The proposed solution shall support URL-Filtering
46	The proposed solution shall support custom URL-categorization
47	The proposed solution shall support customizable block pages
48	The proposed solution shall support logs populated with end user activity reports for site monitoring within the local solution
49	The proposed solution shall support Drive-by-download control
50	The proposed solution shall support URL Filtering policies by AD user, group, machines and IP address/range
51	The proposed solution shall support Vulnerability, Virus and Spyware Protection features across Web and Mail. The solution should support protection against spear phishing attacks
52	The proposed solution shall block spyware and malware
53	The proposed solution shall block known network and application-layer vulnerability exploits
54	The proposed solution shall block buffer overflow, DoS/DDoS , etc type of attacks
55	The proposed solution shall perform stream-based Anti-Virus and not store-and-forward traffic inspection
56	The proposed solution shall perform stream-based Anti-Spyware and not store-and-forward traffic inspection
57	The proposed solution shall support attack recognition for IPv6 traffic the same way it does for IPv4
58	The proposed solution shall support Built-in Signature and Anomaly based Vulnerability Protection Engine
59	The proposed solution shall support the ability to create custom user-defined signatures
60	The proposed solution shall support granular tuning with option to configure overrides for individual signatures
61	The proposed solution shall support automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)
62	The proposed solution Vulnerability / Virus / Spyware protection updates shall not require reboot of the unit.
63	The proposed solution shall support several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc.
64	The proposed solution shall support file identification by signature or file extensions
65	The proposed solution shall support identification and optionally preventing the transfer of various files (i.e. MS Office, PDF, etc.) via protocols like HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, FTP etc.
66	The proposed solution shall support compressed information stored in zipped format and be able to unpack and filter per policy

S/N	Minimum Requirement Specification
67	The proposed solution shall support authentication services for user-identification using any of the following technologies AD, LDAP, eDirectory, Radius, Kerberos, Client Certificate without any additional licensing policy
68	The proposed solution should support the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP
69	The proposed solution shall support user-identification in policy without installing an agent on individual endpoints
70	The proposed solution shall populate and correlate all logs with user identity (traffic, IPS, URL, data, etc.) without any additional products or modules in real-time
71	The proposed solution should support the ability to create QoS policy on a per rule basis specifically by Applications e.g. Skype and Static or Dynamic Application Groups , such as P2P , IM groups
72	The proposed solution should support real-time prioritization of voice based protocols like H.323, SIP, SCCP, MGCP and applications like Skype
73	The proposed solution shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. i.e. Banking, shopping, health and non-personal traffic
74	The proposed solution shall support IPSec, SSL VPN and should be available without additional licensing policy
75	IPSec VPN should be integrated with the proposed solution and support full encryption standards suites: <ul style="list-style-type: none"> <li>- DES, 3DES, AES</li> <li>- MD5 and SHA-1 authentication</li> <li>- Diffie-Hellman Group 1 , Group 2 and Group 5</li> <li>- Internet Key Exchange (IKE) algorithm</li> <li>- AES 128, 192 &amp; 256 (Advanced Encryption Standard)</li> </ul>
76	The proposed solution administrative module shall support the following authentication protocols: <ul style="list-style-type: none"> <li>- LDAP</li> <li>- Radius (bidder specific attributes)</li> <li>- Token-based solutions (i.e. Secure-ID)</li> <li>- Kerberos</li> </ul>
77	The proposed solution shall support packet captures based on Source Address, Destination Address, Applications, Unknown Applications, Port, Threats, Data Filters and / or any combination as specified
78	The IPS should be constantly updated with new defences against emerging threats
79	Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related
80	A minimum storage capability of 2TB (should be on a separate management appliance) need to be provided as part of the solution for logging and reporting
81	The proposed system should have option for creating customized reports. The reports should be accessible through Http/Https based.
82	The administration software must provide a means of viewing, filtering and managing the log data
83	The proposed system must have support for sending log information to an external log server via an encrypted connection
84	Additional components (hardware, software, accessories etc) if required, for providing the total solution as mentioned in the RFP document should be specified and quoted.

S/N	Minimum Requirement Specification
85	Five years comprehensive warranty from OEM (Proof of the warranty must be attached) with onsite service support from the date of installation without any extra cost.
86	Five years comprehensive support for software upgrades for all the major and minor releases
	<b>OEM Criteria</b>
87	The Firewall solution offered must be rated as “leaders” in the latest Magic Quadrant for Enterprise Firewall published by Gartner.
88	OEM must have India presence for last 5 years on both Sales and Support operation.
89	The proposed OEM must have completed NSS Labs’ NGFW Methodology testing with a minimum exploit blocking rate of 95% and must have a track record of continuous improvement in threat detection (IPS).
90	The OEM should ensure that the solution should be operational for 5 years, with all core feature / functionalities enabled on the platform.

#### 7.14. AAA

S/N	Minimum Requirement Specification
1	The proposed solution shall meet the below specifications. Any hardware/software/ licenses required to enable the functionality shall be provided from Day 1
2	The solution must support Authentication, authorization, and accounting (AAA) protocols RADIUS and TACACS+
3	Shall provide authentication, user or administrator access, and policy control for centralized access control. The solution must support an integrated user repository in addition to integration with existing external identity repositories such as Microsoft Active Directory servers, LDAP servers.
4	Offered solution must support scalable AAA services (authentication, authorization, and accounting) including access policy management with a complete understanding of context, such as authentication protocol, user’s role, device attributes, location, and time of day etc.
5	The solution must support authentication protocols like PAP, MS-CHAP, EAP-MD5, PEAP and EAP-TLS.
6	Offered solution shall support use of multiple authentication protocols concurrently.
7	Offered solution shall support multiple identity stores such as Microsoft Active Directory, Kerberos, LDAP-compliant directory, Open Database Connectivity (ODBC)-compliant SQL database, token servers, and internal databases across domains within a single policy
8	Offered solution shall provide TACACS+ server for secure authentication of device administrators, operators etc. with varied privilege levels. It should keep a track of the changes made by the logged-in user.
9	Shall provide automatic detection and categorization of endpoints for security and audit demands, regardless of device type, using contextual data and use this data for optimizing access policies
10	Shall support identify device profile changes and dynamically modify authorization privileges.

S/N	Minimum Requirement Specification
11	Shall support passive device profiling methods such as DHCP, Span Ports, HTTP User-Agent, MAC OUI/Auth or TCP SYN-ACK handshakes
12	Shall support Support active device profiling methods such as SNMP, Subnet Scan, SSH and NMAP Scan
13	Shall support user as well as device authentication based on 802.1X, non-802.1X, and Web Portal access methods across multi-vendor wired networks, wireless networks, and VPNs.
14	Shall support identifying non-802.1x devices as known/unknown type.
15	Shall provide features to define different access levels for each administrator and the ability to group network devices to enforce and change of security policy
16	Shall provide for defining sets of ACLs that can be applied per user or per group for layer 3 network devices like routers, firewalls and VPNs
17	Shall support HTTP/RESTful API's, syslog messaging and Extensions capability to exchange endpoint attributes with firewalls, SIEM, endpoint compliance suites and other solutions for enhanced policy management
18	Shall support integration with SDC 2.0 helpdesk software
19	Shall provide utilities for interactive policy simulation and monitor mode for assessing the policies before applying to the production network
20	Shall support process inbound threat-related events (which are Syslog events received from any third-party vendor device, such as Firewall, SIEM) and perform enforcements and actions based on the defined enforcement policies and services.
21	Shall support customizable Reporting with manual or scheduled reports in PDF/CSV/HTML formats, inventory dashboard showing details of learned devices, real-time monitoring of access requests and events, proactive alerts through Email/SMS
22	Offered solution shall be based on hardware appliance and solution must be deployed with 1:1 redundancy.
23	The solution must support a web-based GUI centralised management for primary and secondary instances. The centralised management must support management of software upgrades on both primary and secondary instances.
24	The solution must include monitoring, reporting, and troubleshooting component that is accessible through the web-based GUI
25	Solution shall be provided with required licenses for minimum 200 concurrent sessions for AAA and TACACS+ access on Day 1. Solution shall be scalable up to 4,00 concurrent sessions without any hardware change.
<b>OEM Criteria</b>	
26	Offered solution shall be Common Criteria certified for Network Access Control (NAC).
27	The AAA solution offered must be rated as leaders or Challenger's in the latest published Magic Quadrant by Gartner for AAA.

## 7.15. DDOS

S/N	Minimum Requirement Specification
1	Solution should be appliance based
2	Minimum 20 Gbps mitigation throughput
3	Total Concurrent Sessions: Min. 10 Million TCP connections
4	Min. 20 Million PPS DDoS Flood prevention rate
5	SSL connection: Min. 33,000 TPS (Key Size of 2048 bit) and 18,000 TPS (ECC Keys) – H/W accelerated
6	Min 18 Gbps SSL throughput
7	< 100 micro seconds latency
8	Ports: Min 8*10G & 16*1G with fully loaded transceivers
9	Management ports: Out of Band 1*1GE Management Port, 1* Rj45 Console Port
10	Deployment modes: Must Support Inline Protection, Out-of-Path Protection and Monitoring mode
11	IPv4 and IPv6 operation and Management from day1
12	Must conform HA between devices with Config Sync
<b>Protection Features</b>	
13	Packet RFC Compliance check
14	Both inbound and outbound DDoS protection
15	DDoS defence based on geographical database
	Should be capable to mitigate and detect both inbound and outbound traffic.
16	Should support Symmetric and Asymmetric Traffic flows.
17	Must have IP reputation feed that describes that describes suspicious traffic blacklisted IPs, Botnet protection and Phishing
	Options for Blacklist and Whitelist, If user wants configurable any customer IPs.
18	TCP Connection Flood Attack Defence
19	Traffic behavioural analysis and protection
20	Auto thresh holding for detection and mitigation of DDoS attacks
21	Real time signature to protect against zero-day attacks including ability to create real time signatures of DNS based attacks.
22	Support BGP Based block-holing.
	Detect misuse of application protocols in the network like HTTP/POP3/STP/SIP/SMTP
23	Protection against DNS flood attack.
24	Capability to do Collaborative DDoS mitigation with automatic signalling to OEM's cloud based DDOS scrubbing Centre upon subscription.
25	Protection from Sophisticated DNS attacks including out of the box mitigation for NX-domain attacks
26	Server stress based L7 Behavioural DOS detection and mitigation including ability to create real time L7 DOS signatures.
27	Custom signature creation.
<b>Reporting &amp; Alerting</b>	
28	Custom Dashboard Creation feature
29	Traffic comparison report

30	IP location wise report
31	Top N attack/traffic/Source Country/IP/etc. report
32	Must support sending alert/report to email
33	Custom reporting template
34	Must support real time packet capture
35	Alarm configuration
<b>Integration</b>	
36	Must Support sFlow, Netflow, Sys logging and SNMPv3 to integrate with external/third party solution
<b>Others</b>	
37	Redundant and Hot Swappable AC PSU, 100-240 VA
38	Must have FCC (part 15, class A), IEC60950-1
<b>OEM Criteria</b>	
39	OEM should be in the Leader's Circle DDOS Solution in as per the latest published Forrester Report

### 7.16. Endpoint Security

S/N	Minimum Requirement Specification
1	Must offer comprehensive customer/server security by protecting enterprise networks from which includes virus protection, spyware, rootkits, bots, grayware, adware, malware and other computer borne threats or mixed threat attacks or any emerging cyber-attacks or zero day attack protection. The solution should be in the of Gartner's leader's quadrant for Endpoint for last 2 years.
2	Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process.
3	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.
4	Must include capabilities for detecting and removing rootkits
5	Must provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution
6	Must have capabilities to restore spyware/grayware if the spyware/grayware is deemed safe
7	Must have Assessment mode to allow first to evaluate whether spyware/grayware is legitimate and then take action based on the evaluation
8	Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process
9	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to:
	a) Terminating all known virus processes and threads in memory
	b) Repairing the registry
	c) Deleting any drop files created by viruses
	d) Removing any Microsoft Windows services created by viruses
	e) Restoring all files damaged by viruses



S/N	Minimum Requirement Specification
	f) Includes Clean-up for Spyware, Adware etc.
10	Must be capable of cleaning viruses/malware even without the availability of virus clean-up components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether.
11	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected customers in case there is an outbreak
12	Behaviour Monitoring :
	a) Must have behaviour monitoring to restrict system behaviour, keeping security related processes always up and running b) Enable certification that a software is safe to reduce the likelihood of false positive detections or equivalent
13	Must provide Real-time lock down of customer configuration allow or prevent users from changing settings or unloading/uninstalling the software
14	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.
15	CPU/memory(physical or virtual) usage performance control during scanning :
	a) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer
	b) Adjusts the scanning speed if:
	c) The CPU usage level is Medium or Low d) Actual CPU consumption exceeds a certain threshold
16	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually
17	Should have Integrated spyware protection and clean-up
18	Should have the capability to assign a customer the privilege to act as a update/master relay agent for rest of the agents in the network
19	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
20	shall be able to scan only those file types which are potential virus carriers (based on true file type)
21	Should be able to detect files packed using real-time compression algorithms as executable files.
22	shall be able to scan Object Linking and Embedding (OLE) File
23	Must provide Web threat protection by the following ways:
	a) Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings
	b) Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location
	c) Must have the capabilities to define Approved URLs to bypass Web Reputation policies
	d) Must provide real-time protection by referencing online database with millions of rated Web domains
e) Configure Web reputation policies and assign them to individual, several, or all end users machine.	
24	Must provide File reputation service

S/N	Minimum Requirement Specification
	a) Must be able to check the reputation of the files hosted in the internet
	b) Must be able check the reputation of the files in webmail attachments
	c) Must be able to check the reputation of files residing in the computer
25	Must protect customers and servers on the network, high performance network virus scanning, and elimination.
26	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users
27	Must have smart feedback to enable feedback from the customer agents to the threat research Centres of the vendor.
	Uses any alternate method other than the conventional pattern based scanning with the following features:
	a) Provides fast, real-time security status lookup capabilities in the cloud
	b) Reduces the overall time it takes to deliver protection against emerging threats
28	c) Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints
	d) Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.
31	Should be able to deploy the Customer software using the following mechanisms:
	a) Customer installation Package (Executable & Microsoft Installer (MSI) Package Format), should support silent installer, unmanaged customers, specific installer for servers
	b) Web install page
	c) Login Script Setup
	d) Remote installation
	e) From a customer disk image
32	Must provide a secure Web-based management console to give administrators transparent access to all customers on the network
33	The management server should be able to download updates from different source if required.
35	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.
36	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console
37	Should have role based administration with active directory integration
	a) To create custom role type
	b) To add users to a predefined role or to a custom role
38	Should have integration with the Active directory 2008/2012 or higher
39	Shall support grouping of customers into domains for easier administration & Endpoint security solution should provide vulnerability protection, which should scan the machine and provide CVE number visibility and accordingly recommend rule for virtual patch against vulnerability.
40	Establish separate configuration for internally versus externally located machines ( Policy action based on location awareness )

S/N	Minimum Requirement Specification
41	Must be capable of uninstalling and replacing existing customer antivirus software and to ensure unavailability of any residual part of the software.
44	Security Compliance should leverage Microsoft Active Directory services to determine the security status of the computers in the network
46	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from customer IPS, customer firewall, and/or network virus logs exceed certain thresholds, signalling a possible attack.
47	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack
48	Should perform Boot & Rootkit scan and cleaning, Endpoint security solution should have capability of AV, Vulnerability protection, HIPS, Firewall, Device control, virtual Patching and integrated DLP with pre and post machine learning execution for malware analysis.
49	Virus definition files should be lighter so that same can be transmitted to remote locations having minimum of 64kbps link or the update pattern size should be less than 200Kb
50	AV should be seamlessly implemented on all the variants of Windows endpoints including Windows XP.
51	System should be configured in such a way that at no case no endpoints/remote agents will be able to communicate with OEM cloud for obtaining updates through internet.
52	In case of bot infection, bot removal tools also to be facilitated to clean the infected machine
53	The solution should have latest machine learning technology in built from day one.
54	The solution should have the option of the endpoint vulnerability shielding in the network.
55	The solution should have ransomware protection in built.
<b>OEM Criteria</b>	
56	Solution should be in leaders in latest published Gartner Magic Quadrant for End Point Protection Platform.

## 7.17. Server Security Solution

S/N	Minimum Requirement Specification
<b>General</b>	
1	The solution must provide a single platform for complete server protection over physical, virtual & cloud.
2	Should provide layered defence against advanced attacks and shields against known vulnerabilities in web and enterprise applications and operating systems.
3	Should prevent access to malicious web sites
4	Should have the capability to Monitor inter-VM traffic and protects Hypervisor.
5	Should protects a wide range of platforms: Windows, Linux, Solaris, HP-UX, AIX, VMware, Citrix, Hyper-V, and Amazon.
6	Should provide self-defending servers; with multiple integrated modules below providing a line of defence at the server: firewall, Anti-Malware, HIPS etc.
7	Solution should have state full Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring and Recommended scan in single module or an in single agent.
<b>Management Console</b>	
8	Proposed solution must have a dashboard to display multiple information.
9	Proposed solution must have a web-based management system for administrators to access using web browsers
10	Management server should have option to install on Windows based server & RHEL server and centralized management for physical, virtual & cloud environment.
11	Management console should provide Firewall Events to view activities on computers with the firewall enabled (typically includes dropped or logged packets).
12	The solution should display exploits detected, either resulting in dropped traffic (Prevent Mode) or logging of events (Detect Mode).
13	Management console should provide System Events to view a summary of security-related events, primarily for the Management server and also including Agents' system events. All administrative actions should be audited within the System Events.
<b>Features</b>	
14	The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites.
15	Solution should have feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.
16	Solution should be ABLE to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.
17	Solution should provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred.
18	Solution should have out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services etc.

S/N	Minimum Requirement Specification
19	Solution should include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits
20	Solution should automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot.
21	Solution should cover of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.) with fine-grained filtering (IP and MAC addresses, ports) and basic prevention of denial of service (DoS) attack
22	Solution should able to detect and protect from reconnaissance scans
23	Solution should be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes.
24	Solution should provide virtual protection which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs/physical servers within minutes.
25	The solution should support Application control, behaviour monitoring & Ransomware protection.
26	The solution should have the capability to integrate with proposed on premises solution for Zero day attack prevention.
27	Solution should support at least Windows Server 2008, 2012, 2016, RHEL, CentOS, Debian, Ubuntu, AIX, HP-UX, Oracle Linux, and SUSE.
<b>OEM Criteria</b>	
28	Offered Solution should be in recommended list as per latest IDC report on Server Security
29	The solution must be certified to Common Criteria EAL 4+.
30	Provides out of the box compliance support for PCI & NIST and OEM should provide engineer (Direct from OEM) with at least 5 working days during implementation.

### 7.18. Vulnerability Assessment Solution

S/N	Minimum Requirement Specification
1	The Solution should Support for centralized administration in a geographically dispersed scanner deployment
2	The Solution should support role-based access and delegated administration for product control and reporting functions
3	The Solution should Integrate with Active Directory or other repositories for role and resource groupings
4	The Solution should have limited/minimal impact on the network
5	The solution shall be capable of consolidating scan data to produce a single report for the entire network/enterprise.
6	Solution must be able to scan hosts, virtual, mobile and security devices for vulnerabilities, misconfigurations and malware using customizable schedules and black-out windows.

S/N	Minimum Requirement Specification
7	Solution must consolidate data from multiple on premises vulnerability scanners and provide remediation trending information.
8	Solution must provide contextual insight and actionable information to prioritize security issues associated with security posture of all enterprise assets.
9	The solution must offer configurable workflows and alerts for administrators to take manual actions via emails, notifications, trouble tickets or take automated actions.
10	Solution must support for organizations that distribute responsibilities across multiple geographies and teams using role-based access control.
11	Solution must provide automated load balancing that help to optimize scan cycles in distributed environments.
12	Centralized vulnerability management with multiple scanners. It must have broad asset coverage like assess servers, endpoints, network devices, operating systems, databases and applications in physical, virtual and cloud infrastructures.
13	Identify weaknesses by scanning traditional assets for known vulnerabilities, misconfigurations and malware
14	The vulnerability management solution must support multiple scanning options, including non-credentialed and credentialed scanning for deep analysis and configuration auditing. It should also support policy based configuration auditing
15	The vulnerability management solution must have agent-based scanning that helps organization to more easily scan mobile and hard to reach assets.
16	Assess how well patch management is working based on vulnerability trends over time
17	Rapidly respond to changes with configurable alerts, notifications and automated actions
18	Measure security posture based on security policies that aligned with high-level business objectives
19	Solution must have feature that help to streamline compliance for the widest range of regulatory/IT standards and best practices
20	Solution must continuously measure the effectiveness of customer-defined security policies based on high-level business objectives to identify and close potential gaps.
21	Solution must have Pre-defined dashboards/reports with automatic feeds from OEM and it should offer highly customizable dashboards/reports, new HTML5- based user interface to satisfy specific needs of CISOs, security management, analysts and practitioners/operators.
22	The Solution should have a feature to change vulnerability or threat ratings (e.g., high, medium, and low, informational).
23	Solution must offer unique report cards that enable Chief Information Security Officers (CISOs) and security leaders to define their security program objectives in clear and concise terms, identify and close potential security gaps, and communicate the effectiveness of their security investments to C-level executives, board members and business managers.
24	Solution must support dynamic asset classification, group assets based on policies that meet specific criteria; e.g., Windows 7 assets with vulnerabilities more than 30 days old.
25	The VM solution must have capabilities for malware detection with built-in threat Intelligence and it should also support anomaly detection using statistical or behavioural techniques
26	The VM solution must detect passive vulnerability of new and "unsafe-to-scan" assets
27	The VM solution must have Real-time detection of botnet and command & control traffic

S/N	Minimum Requirement Specification
28	Solution must be supplied with at least 2048 IP address from day one
29	The solution should support ability to perform web application scanning and should scan configurations, vulnerability checks and report on web applications.
30	The solution should identify susceptibility to database-specific risks, including SQL injection, buffer overflow, and malicious or insecure PL/SQL code.
31	It should check for vulnerabilities in web platforms such as Microsoft IIS, Apache, WebSphere, Novell etc.
32	The Solution should be able to set the entry URL, path to include/exclude and parameters to exclude during a web application scan.
33	The solution should scan for OWASP web application vulnerabilities and for weak input checking and configuration mistakes.

### 7.19. Cloud Management & Orchestration Solution

S/N	Minimum Requirement Specification
1	<p>The solution should support integration with VMware, Hyper-V, RHV, KVM and OpenStack platforms to automate delivery of virtual compute, virtual storage &amp; virtual networking services. All server vendor should provide utility or tool to enable bare metal server provisioning through automation tool or via lifecycle management software.</p> <p>It should also support leading public cloud service provider like AWS, Azure and GCP minimum.</p> <p>The offered software should be open standard with L1-L3 based 24x7 support from OEM, updates and upgrades for the project period. The OEM should have a support centre based out of India with minimum 300 support personal for easier and faster communication on any support call resolution.</p> <p>The solution should have capability to build service catalogue and should be offered with self-service provisioning capabilities.</p> <p>The solution should have resource pool management capability</p> <p>The solution should have metering &amp; integration with chargeback and show back solutions.</p> <p>The solution should provide user authentication and authorization integration capabilities with AD/LDAP provided by OCAC.</p> <p>The solution should provide role base access control using standard authentication and authorization.</p> <p>Access Control interface for all cloud services should be same.</p> <p>The solution should be able to automate and provision data-Centre services such as compute, storage &amp; networking.</p>
2	Cloud Management Platform should support multi-site deployment architecture
3	The solution should support deployment on open, extensible architecture with multi-vendor hardware support.
4	<p>The solution should be able to provide auto scale cloud resources based on resource utilization of VMs.</p> <p>The solution should able to provision and de-provision of resources based on date and time.</p>

	Solution should support for provisioning of Bare Metal servers as a service and bare metal server configuration management.
5	The solution will be able to manage Multi-tenant landscape in the delivered OpenStack.
	A self-service portal is needed to establish a central point of access. The portal should be configurable and accessible via web browser and mobile devices (native or web responsive app).
	Dashboards must be available to allow different customer to control the behaviour and consumption of the services
	All the users should able to access clouds services always through a Single Web Portal
	The solution should provide configuration of approval flows.
	The Solution should allow to define roles and grant permissions to users to access resources at different granularity levels via LDAP/AD.
6	The solution should integration with Configuration Management Tools to manage & configure servers, networks, storage and applications using Chef/Puppet/Ansible Tower/Nagios etc.
	The solution should support Automation and Orchestration via both portal and API.
	The solution should support policy-based orchestration with API support
	The solution should able to integrate with third-party Monitoring and alerting tools via RestAPI or any other methods available.
7	The solution should provide support for Software Defined Networking and auto provisioning of networks.
8	The solution should provide Policy-based Management i.e. it must include a policy engine to ensure cloud resources and services are managed in accordance with organization policies
	The solution should include logic to track and manage compliance with regulatory and industry mandates of the server with API/Tools.
9	The solution should have Service Catalogue for the cloud services and same can be customized.
	The solution should have Life Cycle Management Work flows: Provisioning, Decommissioning, Horizontal Scale, Upgrade etc.
10	The solution should provide forecasting spend associated with currently deployed cloud resources and services.
11	The solution should have ability for work flows to include business approvals
	The solution should have capabilities around Configuration and Change Management work flows
12	The product has capabilities and mechanisms to migrate workloads across the different clouds
	The solution shall check continuously the load of those resources configured as scalable
13	The Solution should have the capabilities for customization of dashboards if required.
	Solution should have ability to provide time period-based reports
	The solution should have capabilities to generate customized reports.
14	Solution should allow access and authorization permission criteria to be linked to role definitions rather than to individual user accounts so that these decisions are driven by a user's membership of a role.
	Solution should support the implementation of Role Based Access Controls (RBAC) for controlling access to resources within cloud.



	Solution should have a feature to grant administrative capabilities to users on a fine- grained manner using integration with AD/LADP etc.
	Solution should provide a powerful logging subsystem that can be used to record and audit the activities requested by customers.
15	The solution will be able to manage Multi tenancy.
16	A portal is needed to establish a central point of access for CMP functions and enable self-service. The portal should be configurable and accessible via web browser and mobile devices (native or web responsive app).
17	Dashboards must be available to allow different customer to control the behaviour and consumption of the services
18	All the users must be able to access all levels of clouds services(IaaS/PaaS) always through a Single Web Portal
19	The solution should have Service Catalogue for the cloud services out of the box and provision to add customized services i.e. addition of new services like IaaS & PaaS
20	The solution should have pre-defined catalogues of templates.
21	The solution should have Life Cycle Management Work flows: Extensible Capabilities to allow "Self-Management" work flows (Reboot/Restart, Migrate/Upgrade, Scale etc.)
22	The solution should manage a broad range of compute, storage and network across cloud platforms
23	The solution should integrate with Software define network (SDN) controllers through API.
24	The Solution should have the capabilities for customization of dashboards and provide customized reports.
25	The solution should allow achieve optimal workload management from initial deployment, ongoing rebalance, to retirement and reclamation with complete lifecycle management.
26	The solution should have capabilities to perform Log retention and Log archival for future access.
27	The solution shall provide a unified management of performance, capacity and compliance for the proposed platform. It should provide the ability to provide ready reports and Dashboard for monitoring purposes with identification capability on over-sized, under-sized, right sizing, Idle and powered-off virtual workloads.

## 7.20. Virtualization Software

S/N	Minimum Requirement Specification
1	The Virtualization software should be based on hypervisor technology which sits directly on top of Hardware (Bare Metal)

	Offered Virtualization software should be open standard with L1-L3 based 24x7 support from OEM, updates and upgrades for the project period. The OEM should have a support centre based out of India with minimum 300 support personal for easier and faster communication on any support call resolution.
2	Virtualization software shall allow heterogeneous support for guest Operating systems like Windows Server, Linux (Red Hat, Ubuntu, CentOS etc.)
3	Should have the capability for creating VM templates to provision new servers
4	Should be able to boot from iSCSI, FCoE, FC SAN
5	Should support VM snapshots to revert back to an older state, if required
6	Should be able to dynamically allocate and balance computing capacity across collections of hardware resources.
7	Should support for cluster services between Virtual Machines.
8	Should support live Virtual Machine migration between two or more servers in a cluster.
9	Virtualization software shall have High Availability capabilities for the virtual machines. The feature should be independent of Operating System Clustering and should work with FC/ iSCSI SAN and NAS shared storage.
10	It should able to restrict placement of a VM to a subset of hosts in a cluster and to keep virtual machines paired or separated.
11	Should provide the capability to live migrate the Virtual Machine files/disks from one storage array.
12	Should allow for creating virtual Networks that connect virtual machines.
13	Hypervisor should have inbuilt Distributed Switch/Bridge/Equivalent to centralize network provisioning, administration and monitoring.
14	Should provide a Web Based Virtualization administrator portal with a graphical management mode for administrators to manage virtual machines, templates, storage, clusters, and Data Centres.
15	Should monitor utilization across virtual machines and should intelligently allocate available resources among virtual machines.
16	Should provide Single-view centralized control of Host and VM system monitoring and management
17	Should have provision for hosts undergoing maintenance to automatically have their guest VMs migrated to other available hosts
18	It should able to provide VM level isolation for better security.

#### 7.21. Openstack Cloud Framework

S/N	Minimum Requirement Specification
1	The entire cloud solution should be based on open standard with L1-L3 based 24x7 support from OEM, updates and upgrades for the project period. The OEM should have a support centre based out of India with minimum 300 support personal for easier and faster communication on any support call resolution.

2	The solution should support x86 hardware from renowned hardware vendor. It should also support standard storage options from different OEM's and native Ceph storage as object mapping.
3	The offered solution should be open-standard and open-source based technologies with enterprise life cycle. The offered solution should be able to scale to hundreds of nodes, automating the whole hardware lifecycle.
4	The solution should be offered with complete feature functionality available with the OEM related to OpenStack Hypervisor
5	The solution should be offered with end to end support of the entire stack: Host OS, Hypervisor, OpenStack including Object storage mapping like ceph. Bidder should offer an integration and supportability matrix with the offered cloud management platform.
6	Should be supported at least lifecycle of 5 years. At least one of the Linux guest flavor which is supported through the lifecycle of 5 Yrs
7	Platform Should be Certified with multiple Industry leading Storage Solutions (At least Ceph, NetApp, EMC, Veritas, HPE etc.)
8	Should be included toolset which helps in Installation, Configuration, Re-configuration, Version management, In place upgrade / update etc.
9	Should be supported Instance high-availability by configuring compute nodes.
10	The proposed solution should support Controller nodes high-availability and load balancing. It should be offered with minimum 3 controllers in high availability, two telemetry nodes and one overcloud node for deployment landscape.
11	Should support Automatic Patch Notification & Security Alerts via lifecycle management software offered. The offered OpenStack solution should support API based deployment management.
12	The solution should support Out-of-the-box Control Plane HA via pacemaker and should support external load balancer.
13	It should be able to create a network file share, available in a Neutron shared network including NFS /CIFS
14	The solution should support SAML federation and authentication with external providers or other clouds
15	It should support multiple disk-formats (QCOW2/ RAW/ ISO/ VDI/ VMDK) and container-format (Bare/ OVF/ AMI/ ARI), checksum and signature verification for extra security
16	Offered solution should support ready state configuration for selected hardware, that automatically configures RAID, BIOS, Network bonding, etc.
17	It should support cloud inventory updates and source control updates and should support scheduled mechanism.
18	The offered solution should be able to deploy different applications in automated and agentless manner in different OS (Windows, RHEL, CentOS etc)

19	The offered solution should support automated multi-tier orchestration tasks to be perform in one or many hosts simultaneously.
20	The proposed solution should support Configuration Management via standard automation tools offered with the solution.
21	Offered hypervisor shall have the capability to create new templates, clone templates from existing VMs to provision VMs
22	Offered hypervisor shall have High Availability capabilities for the VMs
23	Proposed hypervisor should conform to Open standards and should support OpenStack cloud platform.
24	The proposed solution should Support Ceph RADOS or equivalent solution for current or future deployment.

### Automation Software

S/N	Minimum Requirement Specification
1	The software should able to deploy any application in any set of OS for automation. The offered automation software should support Configuration Management and Application Deployment
	The offered software should be open standard and open source in nature with L1-L3 based 24x7 support from OEM, updates and upgrades for the project period. The OEM should have a support Centre based out of India with minimum 300 support personal for easier and faster communication on any support call resolution.
	The software should support tasks to be perform in one or many hosts simultaneously. The automation software should support Multi-tier Orchestration
	The software should be agentless and communication using simple SSH.
	The software should have defined playbook for doing repeated tasks in automated manner. Offered software should be offered with Yet-Another-Markup-Language capability
2	The automation software should have dashboard for providing heads-up NOC-style display for everything going on in your automation environment. it should show host and inventory status; all the recent job activity and a snapshot of recent job runs.
3	Solution scripts should run stream in real time. Automates across to play and tasks complete, broken down by each machine, and each success or failure, complete with output, queue view, source control updates or cloud inventory refresh.
4	The software should able to log activities securely and the same should be viewable later on. The same should support export facility also via API connects.

	It should support audit trail of all changes made to automation tool itself - job creation, inventory changes, and credential storage, all securely tracked.
5	Automation status via integrated notifications should be available. it should able to notify a person or team when your job succeeds, or escalate when jobs fail. The same should able to send notifications across organization at once, or customize on a per-job basis. The same notifications should able to SMS, email, and more - or post notifications to a custom webhook to trigger other tools in your infrastructure.
6	It should support cloud inventory updates, and source control updates and should support scheduled mechanism. It should able to setup occasional tasks like nightly backups, periodic configuration remediation for compliance, or a full continuous delivery pipeline with just a few clicks.
7	It should help to manage entire infrastructure and able to pull inventory from public/private cloud providers such as Amazon Web Services, Microsoft Azure, and more.
8	It should have inbuilt portal mode and survey features to delegate automation job runs to users across the organization - synchronized directly from corporate directories such as LDAP, Active Directory or delegated SAML authentication. With delegation, developers or QA departments should able to provision their own dev and test environments. Customer service agents can provision a new demo environment or junior admins can run simple jobs - like changing passwords - all at the press of a button.
9	The software should support system tracking to audit and verify that machines are in compliance. It should help to discover how a machine has changed over time, or compare machines in running cluster to see how they are different.
10	It should support REST API and CLI for integration with other tools
	The offered automation software should support containerized deployment to scale at runtime as needed
	The offered automation tool should provide mapping of organizations and teams from SAML attribute, configuration of two-factor authentication with SAML, use for multiple LDAP servers within the software
	The offered software should work as OAuth2 provider, allowing easier integration with third party applications for automation.
	Offered software should able to cache isolated node facts and resynch at next connects.

## 7.22. Platform as a Service

S/N	Minimum Requirement Specification
-----	-----------------------------------

1	The platform shall have capability to run both stateful and stateless applications. It should be enterprise Kubernetes based orchestration for managing the platform.
2	The platform shall provide container runtime, container orchestration, container management and container monitoring capabilities.
3	The container platform shall support deployment and orchestration of multiple containers formats (docker,cri-o etc) for preventing any technology lock in.
4	The platform shall have inbuilt management and monitoring capabilities. It should be offered with suitable container registry capability.
5	The platform shall have inbuilt automated application container build capability – from source code to a runnable container image.
6	The platform shall have / support integration with CI / CD tools. Integrated CI / CD tools has to be part of solution.
7	The platform shall support polyglot technologies as runtime platforms for applications such as – Java, PHP, Python, Ruby, Perl, Node.js, Mysql, PostgreSQL, MongoDB, MariaDB etc.
8	The platform shall provide auto scaling capability for automatically running appropriate number of container instances as per load requirements.
9	The platform shall provide auto scaling of application/compute nodes as per load requirement.
10	The platform shall provide container instance auto healing capability.
11	The platform shall provide application / container version management, auto build of new application container instance in test environment basis on application code new version commit. Roll back to earlier version.
12	The platform shall provide deployment strategies support such as – green / blue, canary etc. for ensuring no/minimum downtime for application updates / upgrades.
13	The platform shall provide centralized logging capability (including applications logs from container instances) for audit, logs analysis & ease of management purpose.
14	The platform shall provide integrated container native persistent storage capabilities PaaS Layer around 200TB Need to be offered.
15	The platform shall be deployable using same product on all types of deployment scenarios i.e. – bare-metal servers, virtualized servers, private cloud, public cloud & hybrid cloud.
16	It should be offered with container scanning capability.
17	It should be offered with Kubernetes Cluster Federation for multiple site deployment.
18	The offered platform shall be capable to execute in place upgrade to newer versions whenever new upgrades are available.
19	The offered platform/product should have minimum of seven years of lifecycle.

20	It should be offered with suitable IDE for developing container-based applications.
21	The solution should support multiple x6x86 based server OEM for bare metal deployment, Multiple Hypervisor like VMware, Hyper-V, RHV, OpenStack and multiple public cloud like AWS, GCP, Azure etc.
22	The solution should be offered for 2 physical servers with 32 core each for application/container deployment for the overall solution landscape with L1-L3 based 24x7 support from OEM, updates and upgrades for the project period. The OEM should have a support Centre based out of India with minimum 300 support personal for easier and faster communication on any support call resolution.

### 7.23. Enterprise Management System

S/N	Minimum Requirement Specification
<b>General requirements</b>	
1	All proposed EMS modules like Network Monitoring, Server Monitoring including Application and Database monitoring and Service Management tools must be from Single OEM.
2	To ensure the proposed software is secure, it should have ISO 27001 and/or ISO 2000 certification from a verification or certification agency which has global recognition.
3	The proposed Alarm Correlation and Root Cause Analysis system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The current performance state of the entire network & system infrastructure shall be visible in an integrated console.
4	The implementation of proposed EMS solutions needs to be done by Premium Authorized Service Partner of the OEM. The bidders need to submit valid certificates as a proof of documentation.
5	Any additional components (hardware, software, database, licenses, accessories, etc.) if required for implementation and execution of project, for providing the total solution as mentioned in the rfp document should be provided by the bidder.
<b>Server Infrastructure Monitoring</b>	
6	The solution should provide both Agent-based and Agent less Monitoring in a single solution architecture – that will allow an organization to choose the level of management required and deploys the right-sized solution to meet those requirements.
7	The proposed solution (hardware and software) provisioned from Day 1 should be able to handle 300 devices and shall be scalable to 1000 devices.
8	The solution should be able to monitor the availability and performance of the servers, business applications, databases, applications using one single solution.
9	The proposed Enterprise Management tools must be able to monitor end-to-end performance of Server Operating Systems & Databases and Should be able to manage distributed, heterogeneous systems – Windows, UNIX & LINUX from a single management station.
10	Should be able to monitor bare metal, Hypervisor, KVM, Open stack, Virtualization environment.
11	Solution should provide a web based Central Monitoring Administration console for management, deployment and configuration of monitoring Agents.
12	Central Monitoring Administration web console should also provide downtime configuration feature to schedule planned outages.
13	The solution should provide self-monitoring and notifications capability via sms, email etc.

14	The system should have context-based analysis and forecasting based on performance data with automated policy deployment with detailed, intelligent monitoring of performance and availability data collection.
15	The solution should support Service Impact modelling with automated Event to Monitor association.
16	The solution should have the ability to automate probable cause analysis by automatically grouping events together based on the time that they occur, the business service that they affect and then relating the two to the normal/abnormal behavior of each performance metrics to identify the likely cause of downtime.
17	The root cause analysis (RCA) should require no manual intervention.
18	It should have capability to perform cross-domain correlation with alarm correlation from Network Monitoring tool, Systems monitoring tool and other domain monitoring tools.
19	Multiple dashboards can be created by each user – giving them a streamlined view of what matters most to them, without the noise.
20	The solution should provide detailed Event and Performance Data reporting capabilities.
21	The solution should have OOTB remediation workflows for scenarios like Disk Full, Host Down, ESX not responding, and DB Tablespace Full etc. which can be triggered manually or automatically.
22	The solution must be able to collect following Server Monitoring Parameters: a. Disk failure/utilization b. CPU Failure/utilization c. RAM failure/utilization d. Event logs e. OS Monitoring f. CPU Utilization g. Disk Utilization h. Cluster Monitoring i. Process Monitoring
23	The monitoring systems should have APIs that allow easy integration with third party tools, for Single consolidated dashboard. These should include: a. SNMP adapters, b. parsing log file, c. TCP/UDP Client Server, d. Windows Event logs, e. REST APIs.
24	It should provide the ability to relate infrastructure topology to business services.
25	The solution should be fully integrated with the proposed service desk to view the root cause of the issue, the business service affected and the CI that caused the downtime from with the Service desk. Post Integration with a service desk tool should be able to view the ticket number in the events data.
26	The monitoring solution should be fully integrated with the proposed CMDB to relate event data to the service models in the CMDB to provide visibility into the business impact of downtime.
	<b>Database Monitoring</b>
27	Monitoring of standard RDBMs like Oracle, MS-SQL, DB2, MySQL, Sybase, Postgres etc. in standalone and cluster mode.
28	The tool should provide ability to easily collect and analyse specific information, including information on: o Buffer pools, Locks and other details about lock resources, Tablespaces / Data files / Log files, Database Usage, Database Errors, Database Status, Database File Group Space Usage Level, Database Mirroring Status, Database Transaction Log Usage Level, Database Transaction State, Server SQL Query Performance, Server Query Tuning, Active Connections. o Microsoft SQL Server Connection Check, Microsoft SQL Server Documents, Mirroring Status, Network Statistics, Processes Blocked, Replication Agent Status, Replication Latency, Transactions Active. o Database Server Status, Server key events, Server CPU Usage by SQL, Server Replication Status, Server Transaction Rate, File group Space Usage.



	<ul style="list-style-type: none"> <li>o Workload metrics such as CPU utilization, transaction throughput.</li> <li>o SQL related performance indicators such as percent sorts in memory, disk-sort rate.</li> </ul>
29	The solution should be able to monitor the performance of all the above database and their instances against the defined performance counters and usage of different system resources.
30	The solution should be able to monitor locks and deadlocks for the instances
31	Should proactively identify database problems before they affect end-users and ensure high availability of mission critical databases.
32	Should monitors SQL statements to identify resource-intensive, inefficient and problematic SQL statements to facilitate SQL query optimization and tuning.
	<b>Network Fault Management</b>
33	NMS should provide integrated fault, performance Monitoring, Configuration & compliance Management together in one tool.
34	NMS should support Industry-leading support for physical, virtual, and SDN-enabled devices like Cisco ACI, VMWare NSX, Viptela, Big Switch Networks, etc.
35	NMS should support out of the box monitoring of at least 3000+ devices from at least 150+ vendors.
36	NMS should provide network Trap Analytics out of the box and should provide diagnostic Analytics providing change-Correlated Performance Views and should show the difference either in either a side-by-side, or line-by-line presentation
37	NMS should have built-in audit and compliance policies for industry best practices/ Gov. regulations like PCI, NIST, NVD and other vendor specific standards.
38	NMS should provide Automate Network Operations and Orchestration
39	The solution shall provide information regarding capacity utilization and error statistics for WAN links.
40	The solution should support IPv4, IPV6 and SNMP v1, v2c and shall support migration to SNMP v3 and/ or latest version to provide added security.
41	The solution should process events using consolidation, filtering, normalization, enrichment, correlation, and analysis techniques. Then it should notify the appropriate IT operations personnel of critical events. Solution should also automate corrective action wherever possible.
42	It shall be able to capture, track & analyse traffic flowing over the network via different industry standard traffic capturing methodologies viz. NetFlow, jflow, sFlow, IPFIX etc.
43	It shall collect the real-time network flow data from devices across the network and provide reports on traffic based on standard TCP/IP packet metrics such as Flow Rate, Utilization, Byte Count, Flow Count, TOS fields etc.
44	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements: a) Capture running configuration; b) Capture start-up configuration; c) Upload configuration; d) Write start-up configuration; e) Upload firmware
45	The proposed fault management solution must able to perform real-time or scheduled capture of device configurations
46	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.
47	The solution must allow topology maps to be created for network areas; it should automatically detect and displays links between devices and any change in particular network elements or links status.
48	The solution must Generate accurate ("as-built") physical Layer 2 and Layer 3 diagrams in Microsoft Visio format with the push of a button.
49	The tool should automatically discover different type of heterogeneous devices (all SNMP supported devices i.e. Router, Switches, LAN Extender, Servers, Terminal Servers, Thin-Customer and UPS etc.) and map the connectivity between them with granular visibility up to

	individual ports level. The tool shall be able to assign different icons/ symbols to different type of discovered elements. It should show live interface connections between discovered network devices.
<b>Network Performance Management</b>	
50	The solution should Collect, analyse and summarize management data from LAN/WAN, MIB-II interfaces, various systems and services for performance management. It should allow identifying trends in performance in order to avert possible service problems
51	The solution should provide Performance of Network devices like CPU, memory & buffers etc., LAN and WAN interfaces, Network segments and VLANs
52	The solution should give user flexibility to create custom reports, on the basis of time duration, group of elements, custom elements etc.
53	The solution should provide web-based reports both near real time and historical data for the systems and network devices and should provide reports through e-mail to pre-defined user with pre-defined interval.
54	The solution should provide Real time network monitoring and Measurement of end-to-end Network/ system performance & availability to define service levels and further improve upon them.
55	The solution should identify how device resources are affecting network performance, document current network performance for internal use and service level agreements (SLA).
56	Executive Summary report that gives an overall view of a group of elements, showing volume and other important metrics for the technology being viewed.
57	The tool should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports
<b>Reporting and Dashboards</b>	
58	System must support a large number of out-of-the-box reports in a wide range of categories - Activity, availability, inventory, etc.
59	System must provide a custom-report generation tool that allows the creation of custom reports via a "drag and drop" web interface.
60	It shall be able to monitor and report on availability, delay of target IP nodes – i.e. router interfaces - and also monitor and provide reports on historical utilization of CPU, memory, bandwidth for Network devices.
61	Top N Utilization, Capacity prediction, Availability, Performance, CPU and Memory utilized, Interface errors, Trend report based on Historical Information, Custom report, SLA Reporting, Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports, Availability and Uptime - Daily, Weekly, Monthly, Yearly Basis.
62	Business owners should have a clear view of the extent of impact to their business services and if need be the reason behind the impact.
63	The IT organization and business stakeholders should be able to view their tickets by business service and impact from the same solution
64	For each section, user should be able to select the time frame to report on data. This could be monthly, quarterly, half yearly, yearly or custom dates
<b>Service Management Framework</b>	
65	The solution should have Service Management documentation/ guidelines in built based on latest ITIL best practices and must be ITIL 2011 Gold-level certified on at least 10+ processes by Pink Elephant for process like Incident management, Problem Management, Change Management, Knowledge Management, Service Level Management, Service Asset and Configuration management, Service Catalogue and Request Fulfilment, etc. The certification copy to be submitted.
66	The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost centre, and user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB.
67	The solution should have a single CMDB across ITSM and Asset Management system.

68	Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.
69	Provide option for approval engine so that any customized applications developed could incorporate the hierarchy, role based, level based ad-hoc approval structure. Include notification and escalation capability if approval is not performed.
70	The solution should have the ability to operate all functionality available in the incident, problem, change, assets etc. via a mobile app on iPhone or Android phone.
71	The support person can interact with the end users through chat in built and add those chat transcripts in the ticket.
72	A virtual bot should be available, which can respond to user requests, immediate via portal, email or mobile interfaces.
73	Should provide for Service Requests Workflows and Fulfilment definitions for commonly used IT/Non-IT services.
74	The solutions should allow effectively creating and managing a shared services catalogue for all service request with flexible entitlement controls. The solution should have wizard / graphical workflow editors allowing definition of new request in minutes – without any programming.
75	Integrates with any underlying service management including Service Desk, Change Management, Service Level Management and CMDB for request fulfilment.
76	Beyond mobile iOS and Android apps, Self Service App should be available on any device with an HTML5 browser.
77	Self Service App should provide a snapshot of your day, displaying your activities feed with upcoming appointments, pending requests, unresolved issues, and alerts from systems you use in your daily work.
<b>Service / Help Desk (Incident and Problem Management)</b>	
78	Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.
79	The solution should provide embedded and actionable best practices workflows i.e., best-practices process & views based upon implementations.
80	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively
81	It should have the ability to search multiple built-in knowledge bases like the incident, problem, and known-error database simultaneously without requiring the agent to search each knowledge base individually.
82	Auto assignment must be based on logic for ticket allocation, Engineers geo-location, availability of engineer; as per shift & as per ongoing repairs for resolution, skillset required for the trouble ticket
83	The tool should integrate with a directory system to enable recording and accessing user records of information with capability to integrate with multiple LDAP.
<b>Change &amp; Release Management</b>	
84	The tool should facilitate the identification of the change type and associated workflow For example: standard, normal, and emergency
85	Change management should have fields to record impact analysis and simulate impact, back-out plans, within the change record
86	The tool should facilitate ability of authorized roles to reject changes For example, status of reject, ability to record reason for rejects notification
87	Change management should be capable of integrating with CMDB to facilitate access to CI attributes and relationships to enable change assessment and authorization
<b>Knowledge Management</b>	
88	The tool should integrate with knowledge management OOB - knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions

89	The tool should allow the creation of different access levels (i.e. Read only, write, create, delete) to knowledge management system
90	The tool should have a powerful search engine to sort, retrieve and search using advanced search options, search content in multiple format, and also search within knowledge records
	<b>Configuration Management Database (CMDB)</b>
91	Should Provide a single shared view of services supporting Service Design, Transition and Operations stages of the lifecycle
92	Should automatically create Service models to describe how IT infrastructure supports business services
93	The CMDB should have built-in drift management capabilities to capture and report on infrastructure drift based on infrastructure attributes like RAM, memory, etc.
	<b>Service level Management</b>
94	Solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management. For e.g. monitors and reports across different KPIs like infrastructure (CPU utilization, disk space), response times , resolution times (eg. incident closed on 2 hours) performance and custom parameters of an enterprise
95	Real-time visualization of service level targets, agreement compliance data, penalties and rewards
96	The service level management (SLM) tool should facilitate creation and maintenance of SLAs, OLAs and Supplier / Underpinning Contracts For example: scope, supplier, contact names, contact method, support hours, service level targets
97	The module should link available support hours to service levels when calculating deadlines as well as suspend SLA calculation for certain criteria – e.g. 'pending information from customer'
98	The service management software should have the ability to tightly integrate (bi-directionally) with enterprise management systems for auto-creation/closing / reporting of events/incidents/trouble tickets
	<b>Data Centre Discovery</b>
99	The solution should be able to do a complete discovery of IT environment across distributed (i.e., physical, virtual, network, application, middleware, storage, databases) and heterogeneous environment and provide a clear and visual mapping of IT infrastructure to business services and should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model.
100	The solution should automatically build visualizations that shows dependency between switches, routers, physical/virtual host, storages, cluster software, business applications and other entities and should use Industry-standard protocols such as WMI, SNMP, JMX, SSH to perform discovery without requiring the installation of an agent.
101	The Discovery solution should come with real-time dashboards that collate and present data that allows organizations to make decision on consolidation, re-use of infrastructure, detecting infrastructure that has never been used etc.
102	The solution should be able to automatically detect software's that are end of support, end of extended support and end of life.
	<b>Network &amp; Server Patch Management, Configuration and Compliance Management</b>
103	The system should be able to clearly identify configuration changes / policy violations / inventory changes across multi-vendor network tool.
104	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements: a) Capture running configuration; b) Capture start-up configuration; c) Upload configuration; d) Write start-up configuration; e) Upload firmware.
105	The proposed fault management solution must able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user- defined standard baseline configuration policy.

106	The proposed system should be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.
107	Solution should map network assets and vulnerabilities detected in a vulnerability scan to the network devices and should provide a dashboard for vulnerability detected and vulnerability patched. Based on identified vulnerabilities, system should be able to download the patches/updates from OEM's website or NVD, validate and deploy them on required systems automatically.
108	The proposed system should also provide end to end change management and approval process automation for any patch or update activity.
109	Using the automatic remediation of common IT tasks, the fix should be handled automatically after the problem is detected and a service desk ticket has been created and recorded.
110	NMS should support 3-Dimensional Compliance Model - Configuration, Software, Running State and provides out of the box Risk Visibility Dashboards of network infrastructure.
111	Should Detect, collect and maintain information about Managed Servers, including packaged, unpackaged software, runtime state, host/guest relationships and more.
112	Defines server build sequences for provisioning, incorporating operating systems, patches, and software policies. Supports Solaris, Linux, and Windows®. Supports provisioning of VMware Hypervisor and Solaris Zones.
113	Identifies server vulnerabilities quickly and easily and reduces the time needed to patch multiple servers. Enables patch policy creation and flexible patch deployments. Supports native patch formats for all major operating systems. Provides out-of-the-box integration with Microsoft® Patch Network and Red Hat Enterprise Linux.
114	Improves automation efficiency by managing remote systems and executing tasks from a command line interface. Also supports Windows PowerShell to provide a command line interface (CLI) to Windows servers.
115	Enables rapid troubleshooting and configurable compliance management by comparing servers to reference servers, most golden reference snapshots, industry best practices, or user-defined scripts. Provides comprehensive compliance dashboard with consolidated servers and cross-tier compliance views.
116	Enables code and application deployment on servers in single or multiple instances without proprietary packaging. Imports files, objects, and scripts to define configuration best practices with graphical user interface (GUI) ordering or deployment and uninstall. Uses a granular permissions model to share applications with developers and administrators.
117	Provides dynamic, real-time, and historical reports into hardware, software, patches, and operations activities in complex, heterogeneous data Centres. Includes out-of-the-box compliance reports and at-a-glance compliance status with actionable links to servers, policies, and other objects. Exports reports to HTML and comma-separated values (CSV) formats.
118	The audit trails should be stored centrally and should be digitally signed to prevent tampering.
	<b>OEM Criteria</b>
119	EMS/NMS OEM must be an industry standard, enterprise grade solution and shall be in the present in Gartner's MQ reports for NPMD and ITSM both for last three years or equivalent leading analysts' reports like IDC or Forrester.
120	Proposed NMS solution MUST have at least 3 deployments in Indian Government/ Public Sector, monitoring & managing 5,000+ network nodes in each of such deployments. Customer names, solution details and OEM undertaking needs to be provided at the time of bidding.

#### 7.24. SDN Controller

S/N	Minimum Requirement Specification
<b>General</b>	
1	The SDN solution shall support centralized management through Declarative Policy Engine or SDN Controller and it shall program all the networking policies consistently across any workload - physical and virtual environments.
2	The SDN Solution shall automate networking policies and service overlay provisioning for the Bare metals, Virtual Machines
3	The SDN Solution shall support widely-deployed and standard VXLAN or equivalent technology for overlay tunnel
4	The SDN solution should support VMs (running on ESXi, KVM / Hyper-V/RHEV) Minimum 2 or more platforms must be supported.
5	The SDN solution should enable integration of third-party network and security solutions through standard REST-APIs or Protocols.
6	The SDN Solution shall support Overlay VXLAN, Geneve or equivalent tunnel
7	The SDN Solution shall support VM mobility to further increase the flexibility, elasticity of deployment and scale-out within and across Data Centres.
8	The SDN solution shall provide flexible options for high performance with consistent networking policies using SDN controller by leveraging technologies like DPDK/SRIOV, Virtio/ OVS, Smart-NICS/TSO/ RSS/ LRO/ VXLAN/ Geneve Offload
9	The SDN Solution shall support port Mirroring options in Underlay/ Overlay
10	The SDN solution shall support Micro-segmentation and port mirroring options for hybrid workloads
<b>Management &amp; Control Plane</b>	
11	The solution shall provide integration with cloud management systems using open interfaces like RESTAPI or equivalent
12	Centralised management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management.
13	In Event of all Centralised management appliances or SDN Controllers fails, the Switching network must function without any performance degradation and with the current configuration.
14	Centralised management appliance or SDN Controller must run in "N + 1 redundancy to provide availability
15	SDN Controller shall be deployed on x86 platform or virtualized on any hypervisor like ESXi, KVM etc. If x86 chosen, requisite hardware has to be included in the solution.
16	Centralised management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPENFLOW/ OVSDDB or equivalent.
17	SDN Management / Orchestrator and SDN Controller both should support high availability architecture during component failures
18	Centralised management appliance or SDN Controller must manages and provision L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager.
<b>Management &amp; Service Assurance</b>	
19	The solution shall support DC Overlay/Undelay Correlation: Underlay Connectivity Test. Centralized management appliance or SDN Controller should provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.

S/N	Minimum Requirement Specification
20	The solution shall support Monitoring of VM/Host Virtual Port Reachability State
21	The solution shall support for SW/ HW-VTEP Connection to other SW/ HW-VTEP
22	The solution shall support Overlay Service Debugging including Centralized Management Appliance or SDN Controller - Single pane of Glass for managing, monitoring and provisioning the entire Fabric and should analyse real-time data including metadata, configurations, policies, device/protocol states & run automated checks for potential errors and misconfigurations
23	The solution shall support Real-Time Overlay to Underlay Correlation
24	The solution shall support Historical Failures Root Cause and Impact Analysis
25	The solution shall support Real-Time Overlay Failures Root Cause Analysis: Configuration Problems SDN controller and SW-VTEP
26	The solution shall support Real-Time Overlay Failures Root Cause and Impact Analysis: Underlay Reachability Problems between SDN controller and SW-VTEP/HW-VTEP
27	The solution shall support Visualisation of DC Overlay Components
<b>Security Features</b>	
28	The SDN solution should offer to Create, change, and manage security policies across all Virtual Networks.
29	Solution must support Micro Segmentation for the Virtualize and Non - Virtualize environment
30	The solution should support VM attribute based zoning and policy
31	SDN Controller should communicate over secure protocol between the controller and the agents
32	The SDN solution shall support granular role-based access control policies and support AAA using Local User authentication/ External RADIUS/External TACACS+
33	The SDN Solution should offer Centrally managed distributed L2-L4 stateful firewall
34	The solution should offer distributed firewall should be able to filter traffic based on logical groupings for Virtualized workloads.

### 7.25. Anti- APT Solution

S/N	Minimum Requirement Specification
<b>General Specification:</b>	
S/N	Minimum Requirement Specification
1	Hardware Appliance must be able to handle minimum of 1 Gbps of traffic capacity for inspection
2	Hardware Appliance should have management port
3	Hardware should have minimum capacity of 1 TB

S/N	Minimum Requirement Specification
4	Proposed solution should have option to search for forensic data on endpoint on demand
5	The proposed Hardware should be rack mountable appliance
6	The proposed solution must be available as on premise physical appliances with sandboxing capability and solution should not send any object and data outside the premises.
	<b>Advanced Threat Detection</b>
7	Proposed ATP solution should perform advanced network detection and analysis of the enterprise's internal/External network data.
8	The proposed solution should have the ability to support out-of-band detection
9	The proposed solution should support to monitor traffic from multiple segments simultaneously on single appliance
10	The proposed solution must be a custom built on premise Anti-APT solution and must not network perimeter security component part devices like UTM and NGFW.
11	Security Vendor must have a Research/Labs organization and this organization must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild.
12	The proposed solution should be able to detect any suspicious communication within and outside of Customer's network
13	The Proposed solution should be able to detect communications to known command and control centres
14	The proposed solution should be able to detect reputation of URL being accessed
15	Solution must have Vendor supplied malware patterns readable and customizable by user and should able to identify all the hosts that are infected of the same threat with ability to identify all the hosts that have connected to the malicious site.
16	Proposed solution should have customized sandboxing and analyse the historical data.
17	The Proposed solution should support at least MS 2008, 2012, 2016 OS for Sandboxing and able to protect from Linux, Android and Mac OS based threats.
18	Proposed endpoint anti-apt solution should have dynamic adversary intelligence from external resources and should show in geographical map
19	Customized sandbox solution should support following operating systems (Win2008, Win 2012 and 2016).
20	Sandbox must have the ability to simulate the entire threat behaviour.
21	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency
22	The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files
23	The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing
24	Proposed ATP solution should out of box integrate with NIPS, FW, Endpoint Security and Server Security for intelligence sharing
25	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple sessions and volume traffic analysis



S/N	Minimum Requirement Specification
26	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.
	<b>Management and Reporting</b>
27	The proposed solution shall support CLI, GUI/Web based administration Console.
28	The proposed solution shall support Remote administration using SSH/HTTPS
29	The proposed solution should provide an intuitive Dashboard that offers real time threat visibility and attack characteristics.
30	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Moment, Asset and data discovery and Exfiltration
31	The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats
32	Proposed Appliance should be supplied with 5 years support including phone support & mail support from OEM.
33	Proposed solution should able to do large file analysis from 1kb to 50 mb atleast
34	The sandboxing solution should use a combination of static and dynamic analysis techniques to unmask cleverly disguised malware. It should detect packed malware and VM-aware ones that alter their behaviour in an artificial environment.
	<b>OEM Criteria</b>
35	Solution should be in the recommend list as per the latest NSS report.

#### 7.26. DLP Solution

S/N	Minimum Requirement Specification
<b>S/N</b>	<b>Minimum Requirement Specification</b>
1	The solution should detect and prevent content getting posted or uploaded to specific websites, blogs, and forums accessed over HTTP, HTTPS. The solution should be able to enforce policies by URL's, domains either natively or by integrated Web Security solution. The solution should be able to monitor FTP traffic should be able to monitor IM traffic even if it's tunnelled over HTTP protocol.
2	The solution should be able to block outbound emails sent via SMTP if violates the policy. Mailbox support should be 3000 from day one.
3	Proposed solution should have direct integration with MTA and should not work itself as MTA to avoid single point of failure for mailing system. Proposed solution should also have its own email mail gateway encryption from DLP OEM solution and email gateway solution so that organization can procure it if required in future
4	The solution should be able to prevent content getting posted or uploaded to destinations (Web, Email domains etc.)
5	The solution should have support for Email DLP
6	The solution should be able to identify data leaked in the form unknown and kwon encrypted format like password protected word document. The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review
	<b>Endpoint Data Monitoring &amp; Protection</b>

S/N	Minimum Requirement Specification
7	The solution should have pre-defined applications and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application. The solution should be able to define the policies for the inside and out of office endpoint machines.
8	The solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies
9	The proposed Solution should notify the end user of a policy violation using a customizable pop-up message with justification fields and should capture content that violates a policy and store it in an evidence repository
10	The solution should monitor sensitive content accessed by cloud storage applications on the endpoint and prevent sensitive data from uploading to the cloud
11	The proposed solution should be able to monitor movement of sensitive data at endpoint through various channels such as Bluetooth etc.
12	Endpoint solution should support 64 bit OS, Mac and VDI ( Citrix and VMWare)
13	Proposed solution should support monitoring or blocking data copied from network file shares to the local drive
14	Proposed solution should control the level of access Windows endpoint users have to network shares and USB storage devices. Access can be set to blocked and read only.
15	The Proposed Endpoint DLP Solution must be able to apply DLP policies to Microsoft RMS encrypted files on Windows endpoints to have better understanding of how RMS is being used by employees to protect sensitive data.
16	Proposed Solution should be able to detect sensitive data in hand written forms and should be able to identify blank forms and filled in forms even if the form is handwritten
<b>Data Identification &amp; Policy Management</b>	
17	The solution should have a comprehensive list of pre-defined policies and templates to identify and classify information pertaining to different industry like Energy, Petroleum industry vertical etc
18	The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file
19	The solution should be able to detect and block encrypted and password protected files without reading the encrypted content.
20	The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders
21	The solution should be able to recursively inspect the content of compressed archives
22	Proposed solution should provide granular fingerprinting and should provide the option of how many of those selected columns you want to match
23	The solution should have capability to detect data leaks over print channel.
24	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.
25	The proposed solution should be able to detect and prevent in safe mode
26	The solution should be able to enforce policies to detect data leaks even through image files through OCR technology.

S/N	Minimum Requirement Specification
27	Proposed Solution should support Import and Export of DLP policies only and not entire configuration so that only policies exported can be imported in other DLP management servers
28	Proposed solution should provide granular fingerprinting and should provide the option of how many of those selected columns you want to match
29	The Proposed DLP Solution must be GDPR Compliant
30	The proposed DLP Solution must be able to detect Data Classification Labels applied by Data Classification partners by reading metadata as well as custom header analysis and should also have classification tool from same OEM
31	Proposed solution should provide creating a single policy covering all vectors along with data discover polices
	<b>Automated Response &amp; Incident Management</b>
32	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation
33	Proposed solution should provide the capability of adding metadata to the incidents to accommodate custom remediation processes
34	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI
35	The incident should display the complete identity of the sender (Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager
36	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator
37	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.
38	The proposed solution should have a user level classification and watermarking tool from the same OEM as DLP solution provider. It should provide an additional layer of user-driven data classification by empowering employees to identify and classify sensitive files and email as they create or handle them. Classification is seamlessly integrated into the user interface of leading productivity applications, such as Microsoft Office and Outlook, enabling employees to effortlessly apply a classification tag. It should enable enterprises to classify newly created content, existing files, and emails in a DLP policy-driven or user-driven manner. Bidder may quote it separately in future as and when organization needs it and can be procured in future if organization requires it later.
39	Role Based Access and Privacy Control
40	The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identity of the user and the forensics of the incident
41	The system should create separate roles for user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint
42	The system should allow a role only to view incidents but not manage or remediate them
43	The system should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents
	<b>Reporting and Analytics</b>

S/N	Minimum Requirement Specification
44	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view
45	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients
46	The reports should be exported to at least CSV, PDF formats
47	The system should provide options to save specific reports as favourites for reuse
48	The system should have lots of pre-defined reports which administrators can leverage
49	The proposed solution should provide Incident Workflow capabilities. Proposed solution should also be able to import policies
50	Proposed solution should have the ability to fetch custom attributes from AD/ERP to aid incident management workflow and should not be done using excel sheets
51	The proposed solution should support the following for analysis: Capture the metadata for further inspection Capture SMTP headers, from and destination IP addresses, date/time
52	The DLP dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected.
<b>Storage (Data at rest)</b>	
53	The system should allow automatic movement or relocation of file, delete files during discovery
54	The system should display the original file location and policy match details for files found to violate policy
55	The proposed solution should also have custom file type detection and should offer scripting for creating custom file type based on metadata and not only on extension
56	The system should support incremental scanning during discovery to reduce volumes of data to be scanned.
<b>OEM Criteria</b>	
57	The OEM should be present in the leader quadrant in latest published report of Gartner's for Data Loss Prevention.
58	The OEM should have own technical support centre in India.

### 7.27. Laptop

Minimum Requirement Specification - Laptops		
S/N	Parameter	Specification
1	Processor	8th Generation Intel® Core™ i5-8365U Processor or higher
2	Mother board / Chipset security features	Integrated with processor .TPM 2.0 (hardware based) and Integrated hardware Diagnostic tool in BIOS.
3	RAM	Minimum 8 GB (1x 8GB) DDR4 Memory
4	RAM upgradability and Slots	Minimum 2 nos. DDR4 Memory slots supporting up to 32 GB or higher

Minimum Requirement Specification - Laptops		
5	HDD	Minimum 1 TB SATA or higher
6	Communication & I/O Ports (Integrated in the laptop motherboard)	Minimum 4 USB ports out of which 2 No USB 3.1 and One USB Type C 3.1 Gen1 , HDMI , VGA, RJ-45, SD 3.0 Memory card reader, Universal Audio port Jack security Lock slot.
7	Keyboard & Mouse	Full size Backlit Keyboard with touchpad
8	Camera	Minimum Integrated HD Webcam with Integrated microphones.
9	Graphics	Integrated Intel HD Graphics
10	Sound Card	Intel High Definition Audio with Integrated stereo sound.
11	Display	Minimum 14.0" FHD (1920 x 1080 ) Anti-Glare, LCD display or higher
12	Battery Type	Minimum 4 hrs. back up
13	Weight	Not more than 2.00 Kg.
14	Wireless & Connectivity	Minimum Integrated Intel Dual Band Wireless (supporting 802.11a/b/g/n and ac) network and Bluetooth v 5.0 or higher.
15	Bluetooth	Minimum Integrated Intel Dual Band Wireless (supporting 802.11a/b/g/n and ac) network and Bluetooth v 5.0 or higher.
16	Power and supply	External AC adapter of same OEM make
17	Operating Systems	Microsoft Windows 10 Professional 64 Bit, with latest Service Pack Preloaded License. Systems Hardware driver should be available in OEM website against the offered model.
18	Certifications (for the quoted model )	For OEM: ISO 14001:2004 For the quoted Model :UL,FCC ,Energy Star 6.0/BIS ; EPEAT India, quoted model ROHS , Windows 10 Professional Operating system, Linux & MIL 810 Std. Certification
19	Carry Case (same OEM make)	Standard Good Quality Carrying Case (Standard or Backpack with OEM Logo)
20	Warranty	5 Years OEM onsite including labor and parts replacement (Battery minimum 3 years warranty). Warranty status must be available in OEM website against the supplied model serial no.
21	Manageability	Laptop System Serial No, OEM Name, Model No, to be programmed into BIOS (CMOS); Same information to be provided in Barcode and pasted on the back cover of the laptop for easy readability.

## 7.28. Desktop

Minimum Requirement Specification - Desktops		
S/N	Parameter	Specification
1	Processor	9th Generation Intel Core i5 9500 or better
2	Chipset	Latest Generation business class Chipset (B360/H370/Q370) compatible with the above processor.
3	Motherboard	Motherboard make from the same Desktop OEM (OEM logo must be embossed in the motherboard).
4	Memory	Minimum 8 GB with support for expansion upto 32 GB or higher.
5	RAM Type	DDR4 with 2666 Mhz or higher.
6	DIMMs & Expansion Slots	2 DIMM slots or higher and minimum 4 PCIe series expansion slots and 2 Nos. M.2 slots.
7	Hard Disk Capacity and optical Drive	At least one single disk of Min 1 TB with 7200 rpm or higher. Minimum DVD R/W drive.
8	Graphics	Integrated Graphics (UHD / 4K).
9	Network	10/100/1000 on-board integrated Network Port.
10	USB / HDMI / VGA Ports (Integrated in the motherboard)	<ul style="list-style-type: none"> <li>Integrated USB Ports : Minimum 8 nos (Min 4 nos of 3.1 Gen-1), out of 8 Nos minimum 4 in front, 4 in back and should be easily accessible.</li> <li>Integrated HDMI Port: Minimum 1 no; should be easily accessible.</li> <li>Integrated VGA and Display Port: Minimum 1 no each; should be easily accessible.</li> </ul>
11	Audio	Integrated Audio controller with Internal speaker
12	Cabinet	Tool less chassis with 16 liters or lesser in volume.
13	SMPS	Minimum 85% energy efficient power supply and should be capable of supporting fully configured PC.
14	Operating System and Operating system supported	Windows 10 Professional 64 Bit. Windows 10 Professional and Linux.
15	Security	Hardware based TPM 2.0, chassis Intrusion switch / Intrusion Sensor with chassis physical security cable lock slot.
16	Monitor / Display	Monitor with LED Backlight with minimum Screen size: 19.5" or higher should have at least 1xVGA, 1x Display port 1x HDMI port CPU & Monitor must be of same OEM make.

Minimum Requirement Specification - Desktops		
17	Keyboard	Standard full size keyboard (Same desktop OEM make)
18	Mouse	Standard USB Optical mouse (Same desktop OEM make)
19	Production Unit, Certification and Compliance	<ul style="list-style-type: none"> <li>• Windows 10 Professional and Linux for the quoted desktop model.</li> <li>• EPEAT India for the quoted desktop model.</li> <li>• ROHS for the quoted desktop model.</li> <li>• Minimum Energy Star 5.0 &amp; TCO Certification for Monitors and quoted Desktop model.</li> <li>• OEM ISO 9001 and 14001 Certified India Unit (Proof of Certification of India unit to be submitted).</li> </ul>
20	Warranty	5 years onsite comprehensive OEM warranty (OEM supplied model warranty must be visible in the website in respect to each product serial number).
21	Manageability	System Serial No, OEM Name, to be programmed into BIOS (CMOS); Same information to be provided in Barcode and pasted on the side of the Cabinet for easy readability.

#### 7.29. Multi-Function Printer (Print, Copy, Fax, Scan)

Minimum Requirement Specification – Multi – Function Printer ( Print, Copy, Scan, Fax)		
S/N	Parameter	Specification
1	Printing Type	Black and White
2	Printing Technology	Laser
3	Scanner Type	Flatbed
4	Memory	Minimum 256 MB
5	Processor Type	Minimum 1200 Mhz or higher.
6	Duty Cycle	Up to 75000 pages (Monthly, A4 Size)
7	Paper Handling Input	Should have minimum 100 sheet input tray, two minimum 250 sheet input trays, minimum 50 – sheet automatic document feeder, minimum 125 sheet face down output bin
8	Print Quality	Up to 1200 x 1200 dpi
9	Duplex Printing	Automatic
10	Media Types	(Letter, Legal, Statement, Executive) Paper (plain, Eco EFFICIENT, light, heavy, bond, coloured,

Minimum Requirement Specification – Multi – Function Printer ( Print, Copy, Scan, Fax)		
		letterhead, pre-printed, pre-punched, recycled, rough); envelopes; labels;
11	Scan Resolution	Up to 1200 x 1200 dpi
12	Monthly Scan Volume	Minimum 500 to 3500
13	Digital Sending Standard Features	Scan to USB device and scan to a network folder : JPG & PDF format
14	Operating System and Operating system supported	Windows OS (all 32- & 64-bit editions), Mac OS, Linux OS, SuSE Linux, Unix etc.
15	Display	Intuitive Colour Touchscreen
16	Connectivity	1 Hi-Speed USB 2.0; 1 Host USB; 1 Gigabit Ethernet 10/100/1000T network; 1 Wireless 802.11b/g/n; Easy-access USB (All necessary compatible ports to be supplied with the MFP)
19	Production Unit, Certification and Compliance	<ul style="list-style-type: none"> <li>• Minimum Energy Star 5.0</li> <li>• OEM ISO 9001 and 14001 Certified India Unit (Proof of Certification of India unit to be submitted).</li> </ul>
20	Warranty	5 years onsite comprehensive OEM warranty (OEM supplied model warranty must be visible in the website in respect to each product serial number).

### 7.30. KVM Switch (IP Based)

S/N	Minimum Requirement Specification – IP Based KVM Switch
1	It should have maximum of 16 ports with 2 remote user's concurrency.
2	It should support minimum of one local user at each switch.
3	It should take control of servers at BIOS Level
4	It should facilitate both in-band & out of band access.
5	It should have dedicated 2 ports to integrate with intelligent power strips to reset power of remote device at port level.
6	Same switch should also support connecting serial devices with RS232 interface through different interface adaptor.
7	Switch should support direct telnet/SSH access to serial devices.
8	Remote console level access of both Servers and serial devices such as routers. Serial adaptor should support supports SSH connections pin out to make connections to Cisco equipment quick and easy without the need for any additional external wiring adapters or special wiring.
9	Should support IPV6
10	It should have facility to integrate with secure management devices. It should support Virtual media enables remote USB connections and support for smart card/CAC readers.
11	Shall have 2 gigabit Ethernet ports and support 10/100/1000Mbps.
12	Virtual Media Support of multiple media including .iso image files
13	Shall have redundant power supplies installed.



S/N	Minimum Requirement Specification – IP Based KVM Switch
14	Switch should have more than one Cooling Fans.
15	19-inch rack mountable design.
16	Browser based Management' for both remote and local using standard browsers on Windows and/or Linux.
17	Should support display resolution of 1600 X 1200 or better at remote.
18	Single window access to all the equipment connected to the switch, equipment access logs, and event history and should send email alerts based on log details as triggers.
19	Absolute mouse synchronization.
20	To connect all the ports of the supplied KVM switches to servers / network elements, the required cables / accessories should be provided.
21	It should support FIPS 140 – 2 encryption module for secured communication.
22	The connectivity between the KVM and servers should be UTP using a compatible server interface module with USB and has to support BIOS level virtual media.
21	OEM must have India presence for last 5 years on both Sales and Support operation.
	<b>Management Console:</b>
22	The management software should provide unified, secure access to KVM, serial and power ports of Data Centre devices via a Web browser.
23	The centralized management software should be installed on dedicated Physical or virtual server having specific operating system providing the administrator to put restrictions onto the server as per policies and manage it.
24	It should support installation on 64-bit Operating System.
25	The software should be supplied with open source editable database.
26	Centralized management software should provide "Hub and Spoke" architecture allows for high availability and distributed access across locations. Hub and spoke architecture based solution for failover and replication of management database across locations both being on Active-Active mode.
27	It should provide policy and security management of users and devices connected to KVM and IPDUs
28	It should be able to assign specific node access to a specific user.
29	It should allow the administrator to access, manage and view all equipment, users and access permissions from a single remote device.
30	It should be able to integrate and manage the Virtual infrastructure.
31	Should allow to integrate the RDP, VNC viewer, telnet and SSH services to access the target servers and network appliances over IP.
32	The Management software should natively integrate with ESX servers, Virtual Centre, Citrix Xen Servers, Microsoft Hyper-V and provide the ability to manage them. It should provide a federated view of the virtual servers
33	The system should easily integrate with the existing security infrastructure, authenticating against our internal or external standards-based services. Integration with LDAP, NT /AD, TACACS+, RADIUS and RSA Secure ID is required
34	It should support Virtual Media Deny, View and Control access policies. Centralized management software will provide Access Control List (ACL) and role segmentation for target equipment including Virtual media access to individual server.
35	Should be able to create unlimited users and allow a minimum of ten concurrent users.
36	It should log user activities (login/logout, connect/disconnect), configuration changes at both appliance and managed devices, and status changes of the connected appliances. All of these logs should be forwarded to a network management system or enterprise notification system via SNMP or Syslog.
37	Shall have security features that enable integration with Active Directory external authentication tools.
38	Flexible session time-outs.

S/N	Minimum Requirement Specification – IP Based KVM Switch
39	It should allow: TCP/IP, HTTP/HTTPS, SSL, DNS, and LDAP/LDAPS through network interfaces.
40	It should be able to do Auto-discovery with devices connected for their availability status, and alarms.
41	Shall have flexible logging and reporting options with audit trails for diagnostics and troubleshooting.
42	Should support FIPS 140-2 appliance compliance and 2048 SSL Certificate.
43	Shall support viewing and management of active user sessions and active ports in real time.
44	Shall support authentication mechanism in active-active mode on a hub and spoke architecture.
45	Should allow clients like Microsoft Internet Explorer 9, 10 or 11 Mozilla Firefox® 45 ESR (32 bit) Google Chrome 53 and Microsoft Edge.
46	OEM must have India presence for last 5 years on both Sales and Support operation.

### 7.31. Data Centre Access Management

S/N	Minimum Requirement Specification
1	The proposed solution should be able to seamlessly integrate with the existing solution and support all the Operating Systems including but not limited to Windows, Linux, UNIX etc.
2	The proposed solution should be able to integrated with applications including but not limited to web applications, thick clients, etc.
3	The proposed solution should be able to integrate with other security solution including but not limited to Firewall, IPS/IDS, etc.
4	The proposed solutions should be able to integrate with databases including but not limited to MySQL, Oracle, MSSQL, Mongo DB, Post gres etc.
5	The proposed solution should be agent based or agentless.
6	The solution should be able to integrate with the proposed enterprise authentication methods – Active Directory, LDAP, RADIUS, TACACS etc.
7	The solutions should be able to authenticate, authorize and provide access control to all network devices such as switches, routers, firewalls, load balancers etc.
8	The solution should have the capability to monitor session activities in real time and should maintain audit logs of the same for servers, databases, network devices, applications etc.
9	The solution must have an inbuilt 2-factor authentication mechanism in the form of Mobile OTP/ Email OTP.
10	The solution should be capable of providing real time dashboard and reporting.
11	The solution should maintain audit trails for all administrative and user access and activities.
12	The solution should have the capability to track privileged identities or privileged account activities distinctively.
13	The solution should contain a password vault, which should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set including special characters that can be used for passwords on each target system.
14	The solution should set unique random value anytime a password is changed.
15	The solutions should provide a single console for all administrative tasks.

S/N	Minimum Requirement Specification
16	The solution should be capable of user and group level access with multi-level administrative access.
17	The solution should be able to restrict usage of critical commands and/or tables for database access through SSH, Database Client utilities (TOAD, SQL developer) on any combination of target account, group or target system and end-user.
18	The solution should have maker-checker control built-in for all administrative functions (password changes, system configuration etc.).
19	The solution can restrict target-account-specific entitlements of end users individually or by group or role.
20	The solution should log all the admin activity and that should be monitored.
21	The solution can restrict end-user entitlements to target accounts by days and times of day.
22	The solution must support parallel execution of password resets for multiple concurrent requests.
23	The solution should be able to integrate with the ticketing tools for Incident/Change management.
24	The solution should archive session recording data to external storage/ media based on time and available space.
25	The solution provides the capability to enable end users to retrieve (or reset) a target-system password only after electronic approval by a designated approver. Approval criteria can be based on any combination of target account, group or target system and end-user identity, group or role, as well as contextual information such as day of the week or time of day(Custom code need to be deployed).
26	The solution should be able to perform auto discovery of privileged accounts on target systems and able to perform two way reconciliation.
27	The solution should be scalable in terms of the system administrators, target systems and the concurrent session.
28	The tool must have the required APIs for integration with GRC, SIEM tools etc. or linkage of change & release tickets while raising access ticket request within the tool by the requestor.
29	The solution should be scalable in terms of the system administrators, target systems and the concurrent session.
30	The solution should integrate with the solutions proposed as a part of the Data Centre Security like SIEM, EMS tool etc.
31	The solution should have the ability to capture activities from hooks on process tabs to hooks on mouse, keys, events etc.
32	The solution should have features, which enables to track the creation, rename, modification and deletion of files or folders in the specified directory on critical servers. In addition, it should send email alerts for these activities.
33	The solution should enable on-board of existing user on the active directory in an automated manner.
34	The solution should have provision via which admin will be able to view and control the end users screen and perform activities with elevated rights remotely.
35	The solution should support large variant of Connector Framework that will support all kind of third party application.
36	The solution should have dynamic reporting Dashboard
37	The solution should support multi-tab feature that should allow users/administrators to open multiple sessions in different tabs in the same window and allow them to switch between sessions as required.
38	It should have the ability to control the end user as soon as they log on to their workstations. Also, should be able to elevate the user to access certain applications and restrict users from accessing required applications as and when required by applying profiles.

S/N	Minimum Requirement Specification
39	The solution should automates various administrative level tasks such as installing Kerberos, configuring files, and restarting services for updating the configuration.
40	The solution should provide Centralized Data Warehouse reporting engine for all data centre Privilege Access Management activities done across multiple access management Sites.
<b>OEM Criteria</b>	
41	The proposed solution should have Sales and 24*7-operation support in India.
42	The proposed solution should have a presence in Gartner quadrant
43	The proposed solution should have 3 Client reference in Government sector

## 8. Project Timelines and Liquidated Damages

SI shall deliver all project activities/milestones/deliverables to the Client as per the timelines stated in this section. OCAC or its authorized representative shall take thirty (30) days to review and provide comments on all respective deliverables. SI shall ensure that all comments provided by the OCAC or its authorized representative shall be incorporated in the final version of all deliverables.

All deliverables indicated in the tables below are indicative only and shall be read in conjunction with the Scope of Work section and Standard Form of Contract of the RFP for detailed requirements. Client or its authorized representative reserves the right to ask for additional information, documents and deliverables throughout the Project.

T0- Represents the Project Start Date (i.e. agreement signoff Date of kick off meeting date).

W- Represents the timeline in Weeks after agreement signoff kick off meeting.

Week	Activity/Milestones	OCAC	Consultant	Successful Bidder	Remarks
L0	Project Award	✓	✓	✓	Issue of Letter of Intent (LOI). Letter of acceptance by successful bidder within 7 days of LOI. Draft MSA will be shared to successful bidder within 10 days of acceptance by bidder.
L0+ 4 Weeks= L1	Project Initiation	✓	✓	✓	MSA to be signed within 1 Month from the date of issuance of LOI and PBG @ 10% of the TCV (Total

Week	Activity/Milestones	OCAC	Consultant	Successful Bidder	Remarks
					Contract Value) to be submitted simultaneously.
T0	Project Kick-off & Mobilization	√	√	√	Kick-off meeting to happen within 7 days from the date of signing of MSA along with all the stake holders; Project plan to be submitted.  T0 = Project Start Date
T0 + 1.5 Months = M1	Preparation & Submission of layout, structural drawing, civil works for approval	√	√	√	Submission of design documents, layout, drawing etc. for statutory approvals and Uptime Institute Design Certification
T0 + 2 Months = M2	Finalization and Approval of the submitted layout etc. and Execution of major civil works	√	√	√	Bidder has to work with OCAC for approval from other statutory bodies. Supply and Installation of Brick work, PCC flooring, Partition work, indoor conduit and cabling work for lighting, raw power and UPS points cabling, Earthing and Grounding work. Bidder to furnish monthly progress report on Completion of all major Civil works.
T0 + 3 Months = M3	Delivery & Installation of Electrical & HVAC high side and low side works and structured cabling low side works		√	√	Supply and Installation of Precision Air-conditioning, VRV/VRF cooling system, Electrical panels, Distribution boards, Track busway system, Fiber cable path system. Bidder to furnish monthly progress report.

Week	Activity/Milestones	OCAC	Consultant	Successful Bidder	Remarks
T0 + 4 Months = M4	Delivery & Installation of Major Electrical Components like UPS & Battery, DG, and Rack & IP-PDU etc.		√	√	Supply and Installation of UPS systems and battery banks, Transformer, Diesel Generators, Outdoor bus trunkings, all electrical outdoor cabling. Bidder to furnish monthly progress report.
T0 + 5 Months = M5	Installation of civil & interior works, safety & security systems and passive network cabling works		√	√	Supply and installation of all civil & interior works like raised floor, carpets, doors, furniture, racks, IPDUs and all safety & security (like Access control, WLD, FSS, Rodent repellent, VESDA etc.) CCTV, monitoring devices (DCIM, Asset Management System, & Visitor Management System) and Passive Network structured cabling. Bidder to furnish monthly progress report.
T0 + 6 Months = M6	Commissioning & Testing of all Non-IT systems (PAT of Non-IT System) & Delivery & Installation of IT Equipment	√	√	√	Bidder to carry out integrated system testing of all equipment and rectify all snags. Consultant to work with Bidder for User acceptance Test sign-off of Non-IT Infrastructure system from OCAC. Supply & installation of Hardware like servers, network devices, storage, firewall, cybersecurity devices and all other IT devices except software licenses
T0 + 7.5 Months = M7	Commissioning & Testing of IT Systems, Cloud and Software solution, integration and	√	√	√	Bidder to carry out integrated system testing of all equipment and rectify all snags. Bidder needs to furnish weekly progress

Week	Activity/Milestones	OCAC	Consultant	Successful Bidder	Remarks
	migration of data & network from existing DC to new DC (PAT of IT System)				report and lay down integration plan, migration plan and User Acceptance Test Plan of IT Infrastructure.
T0 + 8 Months = M8	Project Sign-Off & FAT (Go-Live of the Project)	✓	✓	✓	Successful Final Acceptance Test of all commissioned IT and Non-IT systems and Issuance of Go-Live Certificate from OCAC.
M8 + 2 Months = M9	ISO Certifications 27001:2015 9001:2015 20000 :2019 27017:2015	✓	✓	✓	Submission of ISO Certifications.
M8 + 5 Years	Operations & Maintenance	✓		✓	Operation & Maintenance period shall be five years from the Go-Live of SDC.

\* - Its Bidder responsibility to insure MSA signoff will be complete within 30 Days from issuing of LOI; else T0 will be treated as Project start date

## 8.1 Liquidated Damages Table

If the Bidder fails to complete the work within the agreed time schedule (Project Time Line) as specified in the Contract Agreement or any extension thereof, OCAC shall recover Liquidated Damage from submitted invoices from the Bidder as per calculation detailed in the table mentioned below. Equipment / work will be deemed to have been delivered / completed, only when it's all components, Parts / all item of works are also delivered / completed. If certain components / items of equipment / work are not delivered in time, the same will be considered as delayed until such time due missing / incomplete parts / item of works are delivered / completed.

S No	Milestone	Severity	Liquidated Damage	Remarks
1	T0+3 Months = M3	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If fail in completion of works and delivery for more than 5 week, letter of Default will be issue for Improvement.
2	T0 + 4 Months = M4	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If fail in delivery for more than 5 week, letter of Default will be issue for Improvement.
3	T0+ 5 Months = M5	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 5 weeks then, payment of equipment delivery will be hold.
4	T0+6 Months =M6	Critical	1.0 % per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 5 weeks then, payment of equipment delivery will be hold.
5	T0+7.5 Months =M7	Critical	1.0 % per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 5 weeks then, payment of equipment delivery will be hold.
6	T0+8 Months =M8 (Project Sign-Off & FAT (Go-Live of the Project)	Critical	1.0 % per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 10 weeks then, OCAC is free to cancel the WO/contract. The remaining part of work will be



S No	Milestone	Severity	Liquidated Damage	Remarks
				completed by OCAC or any agency engaged by OCAC at the cost of selected vendor.

**Note:**

- The recovery against aggregated liquidated damage shall not exceed 10% of the total contract value (TCV).
- In case bidder fails to complete all the mentioned certification in the RFP within 6 months, after expiration of the mentioned period a penalty of 1% of consolidated certificate cost will be charged per week.
- T0 date of Kick off will be treated as project start date. Total time for the completion of the project: OSDC 2.0 will be 10 months. In case, the Installation, Commissioning, Testing and FAT and Go- Live is not executed within the time, LD will be imposed on the successful bidder as per LD Table mentioned above.

## 9. Payment Schedule

Payment will be released to the successfully shortlisted bidder in phased manner as stated below:

<b>Deliverables/Milestones</b>	<b>Timelines</b>	<b>Payment</b>	<b>Remarks</b>
Inception Report / Mobilization Advance	T0 + 1.5 Months	5 % of total capex quoted value	Submission of Design document, Shop drawings, Uptime design document for certification, coordinated drawings, Project plan, Resource deployment plan, Engagement of Project Manager at site.
Execution of major civil works	T0 + 2 Months	5 % of total capex quoted value	Supply and Installation of Brick work, PCC flooring, Partition work, indoor conduit and cabling work for lighting, raw power and UPS points cabling, Earthing and Grounding work.
Installation of Electrical & Cooling system high side & low side Components.	T0 + 3 Months	10 % of total capex quoted value	Supply and Installation of Precision Air-conditioning, VRV/VRF cooling system, Electrical panels, Distribution boards, Track busway system, Fiber cable path system. Confirmation Letter /Mail from respective OEM & Delivery Certificate.
Installation of major Electrical Components	T0 + 4 Months	10 % of total capex quoted value	Supply and Installation of UPS systems and battery banks, Transformer, Diesel Generators, Outdoor bus trunkings, all electrical outdoor cablings. Confirmation Letter /Mail from respective OEM & Delivery Certificate.
Installation of civil & interior works, safety & security systems and passive network cabling works	T0 + 5 Months	10 % of total capex quoted value	Supply and installation of all civil & interior works like raised floor, carpets, doors, furniture, racks, IPDUs and all safety & security (like Access

			control, WLD, FSS, Rodent repellent, VESDA etc.) CCTV, monitoring devices (DCIM, Asset Management System, & Visitor Management System) and Passive Network structured cabling. Confirmation Letter /Mail from respective OEM & Delivery Certificate.
Commissioning & Testing of all Non-IT systems (PAT of Non-IT System) and Supply & Installation of major IT components of OSDC 2.0	T0 + 6 Months	25 % of total capex quoted value	Supply & installation of Hardware like servers, network devices, storage, firewall, cybersecurity devices and all other IT devices except software licenses. Confirmation Letter /Mail from respective OEM & Delivery Certificate.
Commissioning & Testing of all IT systems, cloud and software solutions (PAT of IT System). Submission of as-build drawing, warranty documents, SOPs, Integration & Migration.	T0 + 7.5 Months	15 % of total capex quoted value	Supply and installation of EMS, endpoint security licenses, cloud solution, submission of software licenses. Confirmation Letter /Mail from respective OEM & Delivery Certificate.
Final Acceptance Test & Go-Live of DC. Engagement of Operation & Maintenance team	T0 + 8 Months	10 % of total capex quoted value	Final Testing and commissioning of individual systems and components, Integrated testing, Uptime certification testing, Go-Live certification and Engagement of Operation and maintenance team.
On successful running of DC for one year from final acceptance test, integration and migration along with submission of requisite documentation.		Final 10% of capex quoted value	The payment will be against submission of Performance Bank Guarantee, 10% of quoted value valid for 1 year.

<p>Operations and maintenance Management for 5 year payable quarterly</p>		<p>25% (per quarter) of the yearly quoted price.</p> <p>1st quarter pay-out will be made post submission of structured cabling certification valid for 25 yrs.</p>	<p>Payment terms would be quarterly in arrears after making due adjustment with SLA/ performance</p>
---	--	--	--

Note: - All the payments will be made to the successful bidder in Indian Rupees only. Payments will be made after thirty (30) days of receiving the invoice subject to approval from competent authority. The billing has to be made in the name of OCAC.

Tax shall be shown extra by the Bidder in their invoices for the items applicable. The same shall be paid by OCAC as per actual after verification. Similarly, if there is any tax savings, the same shall be reduced from the payable amount.

In case of any new incidence of tax or any change in existing tax rates taking place during the Agreement Period, that shall be borne and payable by OCAC over and above the agreed price for each item as may be applicable as per the Invoice raised by either Party/Member of the on OCAC. Similarly, any reduction in taxes shall be to the benefit of OCAC. All invoices produced to OCAC for payment should be with TAX invoice.

The percentage of the operational expenditure (OPEX) should not be less than 30% of the total quoted value.

**CAPEX** may include the cost of Non-IT, IT equipment, active and passive component required for OSDC 2.0 (Year 0 Cost).

**OPEX** may include operational expenditure as Manpower cost, and Annual maintenance cost of all the equipment's for 05 (Five) years (Year 1+ Year 2+ Year 3+ Year 4+ Year 5) etc. to be incurred by the bidder for operation and maintenance of OSDC 2.0 for 5 years after Go-Live.

## 10. Service Level Agreement

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof to be offered by Bidder to OSDC. The Bidder shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels to provide quality services. The Bidder shall meet service level objectives and corresponding parameters to ensure the delivery and quality of services on time as per standard mentioned in the document. Service level indicators & and the target performance levels to be maintained by the Bidder during the contract period. SLA shall be strictly imposed and agency shall be deployed for reporting the performance of the Bidder against the target performance metrics. All logs, reports and data that shall be made available for the purpose of evaluation/audit of SLA parameters/target performance metrics should be system generated only.

The benefits of this SLA are to:

- ✓ Trigger a process that applies Customer and the Bidder management attention to some aspect of performance when that aspect drops below an agreed upon threshold, or target.
- ✓ Makes explicit the expectations that Customer has for performance.
- ✓ Helps Customer to control the service level and performance of Bidder services.

The Bidder shall have to submit a quarterly report to monitor the performance of the services being provided by the Bidder and the effectiveness of this SLA

### 10.1 Brief Description of the Services to be provided

The Bidder will provide following services for Site Preparation & Supply, Installation and Maintenance of basic Infrastructure for the establishment of State Data Centre at the proposed site. The exact scope and boundaries of services provided as part of this Contract are detailed in Detail Scope of Work therein of this RFP.

- ✓ Site Preparation of the proposed Data Centre in terms of the civil, electrical and mechanical work required to Build and maintain the Data Centre.
- ✓ Supply, installation and setting up of the necessary basic Infrastructure (state of Art UPS and Air-conditioning System, Transformer, Fire management, Lighting system, Fire Detection and Control system, Structure Cabling, etc.).
- ✓ Supply, installation and setting up of the physical security system and CCTV surveillance systems.
- ✓ Five years on-site maintenance of all the equipment's and their components supplied in setting up the basic Infrastructure in the proposed Odisha State Data Centre.
- ✓ Onsite support for Data Centre Infrastructure Operations on 24\*7\*365 basis by skill manpower / Personnel for a period of five years to ensure 99.982% availability

### 10.2 SLA Definitions

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings set forth below:

- ✓ **"Availability"** shall mean the time for which the services and facilities offered by the Bidders are available for conducting operations from the equipment hosted in the Data Centre.
- ✓ **"Downtime"** is the time the services and facilities are not available to Customer, which excludes the scheduled outages planned in advance for the Data Centre.
- ✓ **"Helpdesk Support"** shall mean the Bidder's 24x7x365 Helpdesk Support Centre which shall handle Fault reporting, Trouble handling, Ticketing and related enquiries during this contract
- ✓ **"Incident"** refers to any event / abnormalities in the functioning of the Data Centre Equipment / Services that may lead to disruption in normal operations of the Data Centre services.
  - **CRITICAL:** Incidents, whose resolution shall require additional investment in component or time or shall involve coordination with OEMs. These incidents shall impact the overall functioning of the SDC. For example, Power failure, failure of Spine switch, etc.
  - **Medium:** Incidents, whose resolution shall require replacement of hardware of software parts, requiring significant interruption in working of that individual component, for example, installation of operating system, replacement of switch, etc.
  - **Low:** Incidents, whose resolution shall require changes in configuration of hardware or software, which will not significantly interrupt working of that component.
- ✓ **"Resolution Time"**, means time taken by the Bidder staff to troubleshoot and fix the problem from the time the call has been logged at the Helpdesk till the time the problem has been fixed.

### 10.3 Category of SLA

This SLA document provides minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The DCO shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels.

The SLA has been logically segregated in the following categories:

- A. Performance Related Service Level
- B. IT infrastructure related service level.
- C. Virtual Infrastructure Related Service Level
- D. Security and Incident Management
- E. Helpdesk Support Services
- F. Manpower related Service Level
- G. Compliance & Reporting Procedure
- H. Civil major and minor Works

### 10.4 Targets of Service Level Agreement

SLA clause provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Bidder shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the

performance levels. The services provided by the Bidder shall be reviewed by the Consultant/PMU and Customer shall:

- ✓ Check performance of the Bidder against this SLA over the review period and consider any key issues of the past period's performance statistics including major incidents, service trends, etc.
- ✓ Discuss escalated problems, new issues and matters still outstanding for resolution.
- ✓ Review of statistics related to rectification of outstanding faults and agreed changes.
- ✓ Obtain suggestions for changes to improve the service levels.

In case desired, Consultant /Customer may initiate an interim review to check the performance and the obligations of the Bidder. The SLA may be reviewed and revised in accordance to the define procedures. The procedures will be used if there is any dispute between Customer and the Bidder on what the performance targets should be.

### 10.5 Performance Related Service Levels

S No	Measurement	Definition	Interval	Target	Target in Time	Penalty
1.	Data Centre Availability	Availability = $\{1 - [(Downtime) / (Total Time - Maintenance Time)]\} * 100$ Availability of Power will be measured upto the socket level in the equipment room that will be providing power to the racks.	Quarterly	$\geq 99.98\%$	25 minutes Continuous downtime	No Penalty
				$\geq 99.75\%$ to $< 99.98\%$	$\leq 30$ minutes to $> 25$ minutes of downtime	0.5% of the QGR value
				$< 99.75\%$	$> 30$ minutes of downtime	For every 0.25% reduction in the uptime there will be a penalty of 2% QGR.
2.	Temperature	The server farm area temperature should be maintained all the time. Temperature log reports should be stored for a period of minimum 4 months.	Quarterly	20 + - 2 Degree Centigrade in the server farm area all the time.	0-4 instances in a week	No Penalty
				20 + - 2 Degree Centigrade in the server farm area all the time.	5 no of instances or more than that in a week	Penalty of 0.25% of the QGR value for [If Instances count more than 10 in one QGR then it

S No	Measurement	Definition	Interval	Target	Target in Time	Penalty
						Record as Event of Default], a letter of warning may be issued to the bidder.
3	Humidity	The server farm humidity should be maintained all the time. Humidity log reports should be stored for a period of minimum 4 months.	Quarterly	The humidity should be within range of 50% +- 5 RH all the time	0-4 instances	No Penalty
					5 no of instances or more than that in a week	0.25% of the QGR value for [If Instances count more than 10 in one QGR then it Record as Event of Default], a letter of warning may be issued to the bidder.
4.	CCTV camera Availability Shall be measured for all cameras installed and NVR	Availability = $\{1 - [(Downtime) / (Total Time - Maintenance Time)]\} * 100$	Quarterly	>= 99.98%	25 minutes	No penalty
				Between 99.98% and 99.75%	<= 30 minutes to > 25 minutes of downtime	0.5% of the QGR value.
				< 99.75%	> 30 minutes of downtime	1% of the QGR value.
5	CCTV Footage Availability	CCTV footage/NVR data should be kept stored for some period of time.	Quarterly	The SI/DCO should maintain the CCTV footage recordings of past 30 days at given point of time. The recordings should be taken back up and store for minimum of 3 months.	30 days with NVR and 3 months with storage.	0.01% of the QGR value plus Letter of Warning to be issued to the bidder.



S No	Measurement	Definition	Interval	Target	Target in Time	Penalty
6.	Availability of Access Control Devices	Availability = {1- [(Downtime) / (Total Time – Maintenance Time)]}*100	Quarterly	>= 99.98%	25 minutes	No penalty
				Between 99.98% and 99.75%	<= 30 minutes to > 25 minutes of downtime	0.5% of the QGR value on an incremental basis.
				< 99.75%	> 30 minutes of Downtime	1% of the QGR value

### 10.6 IT Infrastructure Service Level

IT Infrastructure service level will be applicable on the devices which are part of the BOM and mentioned at Annexure-

10.6.1 Servers and Systems as mentioned in Table of Annexure

10.6.2 Storage and Backup Devices as mentioned in Table of Annexure

10.6.3 Network Devices as mentioned in Table of Annexure

10.6.4 Safety, Security and IT support Equipment's as mentioned in Table of Annexure.

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	Individual Server Availability (including the OS, database and the application running on it)	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning may be issued to the bidder.
2	Storage Availability	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system

Sl. No.	Definition	Measurement Interval	Target	Penalty
				[Record as Event of Default] Letter of warning may be issued to the bidder.
3	<p>Managed Backup Service Availability (with agreed retention period)</p> <p>Managed Backup Service provides automatic scheduled backup of Customer Data to the designated storage vault 'as is where is' and also restore it back in the same format as backed-up.</p> <p>Data backup Success Ratio must be calculated.</p>	Quarterly	$\geq 99.98\%$	No Penalty
			$\geq 99.97\%$ to $< 99.98\%$	0.1% of the QGR value for O&M of IT system
			$\geq 99.96\%$ to $< 99.97\%$	0.25% of the QGR value for O&M of IT system
			$\geq 99.93\%$ to $< 99.96\%$	0.5% of the QGR value for O&M of IT system
			$< 99.93\%$	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning may be issued to the bidder.
4	Connectivity with Internet (With regards to OSDC equipment only)	Quarterly	$\geq 99.98\%$	No Penalty
			$\geq 99.97\%$ to $< 99.98\%$	0.1% of the QGR value for O&M of IT system
			$\geq 99.96\%$ to $< 99.97\%$	0.25% of the QGR value for O&M of IT system
			$\geq 99.93\%$ to $< 99.96\%$	0.5% of the QGR value for O&M of IT system
			$< 99.93\%$	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning may be issued to the bidder.
5	LAN availability (Active and passive components)	Quarterly	$\geq 99.98\%$	No Penalty
			$\geq 99.97\%$ to $< 99.98\%$	0.1% of the QGR value for O&M of IT system
			$\geq 99.96\%$ to $< 99.97\%$	0.25% of the QGR value for O&M of IT system
			$\geq 99.93\%$ to $< 99.96\%$	0.5% of the QGR value for O&M of IT system
			$< 99.93\%$	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning may be issued to the

Sl. No.	Definition	Measurement Interval	Target	Penalty
				bidder.
6	<p>Preventive Maintenance</p> <p>DCO shall provide a detailed Preventive maintenance plan/Schedule on commencement of the Project.</p>	Quarterly Reporting	100% Carried Out. PM Plan should be Approved from PM, OSDC/OCAC prior to be carried out in that quarter.	<p>2% of the QGR value for delay in PM activity.</p> <p>0.1% of the QGR value for non-adherence to PM plan or without approval.</p> <p>If PM of any equipment missed in a quarter, the same should be carried out within next two weeks. Else penalty of Rs. 5000/- per day per equipment for delays will be deducted.</p>

## 10.7 Virtual Infrastructure related Service Levels

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	Provisioning and De-Provisioning of Virtual Machines	Quarterly	Within 1 Hour after the approval of the request by the Customer/ User	0.5% of the QGR value for O&M of IT system for more 1 hours of delay beyond the target time. To the maximum capping of 5 hrs  1.0 % of the QGR value for O&M of IT system for more 5 hours of delay on an incremental basis.
2	Overall Cloud Solution Availability (includes cloud network, cloud virtualization layer, cloud storage, virtual OS, cloud orchestration layer, cloud security layer and any other requisite component and services)	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning may be issued to the bidder.
3	Production Cloud or Cloud Dashboard is down, business operations severely impacted with no workaround; or a security issue	Every instance in the Quarter	Up to 25 minutes	No Penalty
			>25 min to <= 1hr in case of peak hour (8 am to 8 pm on weekdays) and > 1hr at any other time	0.5% of the QGR value for O&M of IT system for 1 <sup>st</sup> time and 0.1 % of QGR value for O&M for IT system for every subsequent lapse.

## 10.8 Security and Incident Management Service Levels

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	For every Virus attack reported and not resolved within 36 hrs from the time of attack	Every instance in the Quarter	Beyond 36 hrs	Rs.20,000.00 for delay of every 24 hours or its part. If more than three virus attacks are reported in a quarter, then 10% of the QGR would be deducted as penalty.
2	For every instance of Denial of Service (DoS) attack and not resolved within 2 hrs from the time of attack.	Every instance in the Quarter	Beyond 2 hrs	Rs.5,00,000.00 per DoS attack
3	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ OSDC data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty.	Every instance in the Quarter	At every instance	Rs.5, 00,000.00 per instance.
4	For every Intrusion reported by firewall or IPS and not resolved within 2 hour from the time of report	Every instance in the Quarter	Beyond 2 hrs	Rs.2,00,000.00
5	Patch Management (including rules updation in Firewall, IPS and updation of any SPAM control policy)	Every instance in the Quarter	Within 2 hrs time from the approved Request	No Penalty
			> 2hrs and <=3hrs	Rs.1,00,000.00
			> 3hrs and <=4hrs	Rs.2,00,000.00
			> 4hrs and <=5hrs	Rs.3,00,000.00
			Beyond 5hrs for every 3 hrs	Rs.5,00,000.00

### 10.9 Help Desk Support Services Level

**Response time:** is defined as the time between receipt of the incidence (helpdesk call/ receipt of alarm generated by management system) and a support team member begins working on the incidence.

**Resolution time:** is defined as the total time between receipt of the incidence (helpdesk call/ receipt of alarm generated by management system) and the incidence been resolved.

**Service Window:**

PWH (Prime Working Hours): 8AM to 8PM (Monday to Saturday)

EWH (Extended Working Hours): 8PM to 8AM (Monday to Saturday), Sunday and all state Government Holidays.

Priority	Response Time	Resolution Time		MAT (Maximum Allowable Time) After Resolution Time.	
		PWH	EWH	PWH	EWH
	<b>PWH or EWH</b>				
<b>1</b>	10 minutes	Within 6 Hours	Within 6 Hours	4 Hours	4 hours
<b>2</b>	20 Minutes	Within 8 hours	Within 12 hours	4 hours	4 hours
<b>3</b>	30 Minutes	Within 12 hours	Within 24 hours	12 hours	12 hours

S NO	Definition	Measurement Interval	Target	Penalty
1.	"Resolution Time", means time taken by the Bidder staff to troubleshoot and fix the problem from the time the call has been logged at the Helpdesk till the time the problem has been fixed.	Quarterly	100% calls to be resolved within 30 minutes	No Penalty
			Calls resolved after 30 minutes of OR Unresolved call	0.01% of the Total QGR value for every call (with the delay of 30 minute) on an incremental basis.

#### Setting Priority Level

The Helpdesk at OSDC will make every effort to resolve issues at the time of the service call. This will be the initial method for resolving issues before assigning a priority level. Helpdesk staff will log and assign priorities for all requests not resolved at the time of the call.

Incident priority is primarily formed out of its Impact and Urgency. The helpdesk will maintain a matrix as per the EMS deployed which will automatically calculate incident severity out of the simple value of Impact x Urgency.

Impact of the incident is the measure of how business critical it is.  
Urgency is a necessary speed of resolving an incident.

### **Priority = Impact x Urgency**

#### **Priority for Critical Components:**

Priority levels for some of the services are given below. OCAC reserves right to define the priority levels of services not mentioned below.

#### **Priority Level-1**

Standard compliance due to total breakdown/ failure of any equipment or component installed in the OSDC. Users, equipment's and services will be covered under this Priority level.

- Access Control Server Failure
- Anti-Virus Server Failure
- Active Directory Failure
- BMS Service Failure
- Backup Server Failure
- Cluster Service Failure
- Controller Failure
- DNS Service Failure
- Directory Service Failure
- Database Failure
- Database Node/ Instance Failure
- Firewall Failure
- Genset Failure
- IPS Failure
- SIEM Failure
- HIP/HIDS failure
- Load Balancer Failure
- LT Panel Failure
- Physical Infrastructure components related to PAC of server farm area
- Physical Infrastructure components related to security of server farm area: CCTV, Physical Access Control
- Physical Infrastructure components related to fire suppression
- Passive cable component connecting the equipment's
- Power Failure to Rack(s)
- PAC Failure
- Router Failure
- RAID Controller Failure
- Switch Failure
- SAN Switch Failure
- Storage Failure
- Server/ System Failure
- Storage Solution Related Issue

- Security Component Failure of Server Farm Area
- Sync Panel Failure
- Tape Library Failure
- UPS Failure
- VTL Failure
- Threshold Alarm (Critical)

**This is an indicative list and not exhaustive.**

**Priority Level-2:**

Standard Compliance due partial breakdown/ failure of any one of the equipment/ component installed in SDC. The indicative list of such incidents/ request is as given below:

- Agent – Installation, Configuration, Modification, Uninstallation
- Backup – New Backup Request, New Policy, Change in Policy, etc,
- Failure of physical infrastructure components related to humidity control and comfort air conditioning other than Server Farm Area
- Fiber optic cable failure
- Failure of modules / slot
- Fabric cable failure
- Firmware Upgrade
- HBA Failure
- IOS – Update, Upgrade, Downgrade
- IDS/ IPS Policy updating as per new requirement
- InfoSec Incidents (IT-Critical)
- InfoSec Incidents (Non IT-Critical)
- NIC failure
- Tape drive failure
- LUN's / Storage Volumes – Allocation, Add to existing, Delete, etc., Issue
- LAN Connectivity as per requirement
- Port Failure
- PSU / Cooling Fan failure
- Passive cable component connecting the above equipment's
- Physical infrastructure components related to security of other area other than server farm
- Signature Update
- Server Reboot Request
- User Account Locked

**This is an indicative list and not exhaustive.**

**Priority Level-3**

Partial / breakdown of any equipment/ component installed in the Data Centre without disrupting any services and failure/ delay in undertaking and completing activities listed below. The indicative list of such incidents/ requests is as given below:

- Adding new device to Fabric.
- OS – Installation, Uninstallation
- Patch – Update, Remove,



- Threshold alarm (Major)
- H/W up gradation
- Antivirus updates
- Printer - Cartridge Change
- Coolant for Genset
- Desk Phone – New Allotment, Shifting,
- Data – Archival, Restoration
- Database – New User Request, Modify user access rights, removal/ disable user.
- Planned Maintenance
- User Management – New User, Removal of User
- Access Card – New Card Request, Issue, Removal / Assigning Rights, etc
- Backup policy
- FTP Service – New User, Password Reset, Access Modification, Removal of User, etc.
- Power failure to PDU
- PDU Requirement
- Patch cord request
- RCA Report
- IP Address – New Request, Removal
- InfoSec Incidents (IT-Non Critical)
- InfoSec Incidents (Non IT-Non Critical)
- Security incident Report\*
- VPN Service – New Request, Issue,
- VNC\ Remote Login – New Request, Issue,
- Printer Issue

This is an indicative list and not exhaustive

**This is an indicative list and not exhaustive.**

## 10.10 Manpower Service Levels

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	Resource availability for all services agreed for Operation and Maintenance purpose of the project. DCO	Quarterly	Single absence of a single resource	No Penalty (if replaced by equivalent skilled resource)

	manpower should be available 24x7x365 days.			Replacement should be subject to prior approval of Project Manager OSDC/ OCAC.
				Double of the cost of the absent resource for the period of absence.

**NB: Minimum no of Resource need to be present in all shift at Data Centre should be not less than 36. (Excluding Holidays)**

The replacement of manpower by bidder after deployment will be allowed (without penalty) only in below cases.

1. The resource leaves the organization by submitting resignation with present employer and a copy of resignation should be marked to OCAC/OSDC.
2. Bidder will withdraw the resource as per its own organization policy in case of non-performance and non-corporation in line with the OSDC guidelines.
3. For Skills and Competence level the resource profile, educational qualification and certifications should be verified by the Consultant and OCAC/OSDC jointly prior to deployment.
4. No resource will be absent without prior permission from the designated authority.
5. A Background Verification may be carried out for selected resources to ensure no criminal history present.

**Details of manpower requirement is as follows:**

Sl.	Role	Working Shifts			
		6:00 AM To 2:00 PM	10:00 AM To 6:00 PM (Monday to Saturday)	2:00 PM To 10:00 PM	10:00 PM To 6:00 AM
1	DC Project Manager	☎	1	☎	☎
2	Network & Security Administrator	☎	1	☎	☎
3	Cloud & Server Administrator	☎	1	☎	☎
4	EMS Specialist	☎	1	☎	☎
5	Database Administrator	☎	1	☎	☎
6	Storage and Backup Specialist	☎	1	☎	☎
7	SIEM Analyst	☎	1	☎	☎

8	Network Engineer	1	-	1	1
9	Server Engineer	1	-	1	1
10	Helpdesk Support	1	-	1	1
11	Facility Manager	☎	1	☎	☎
12	BMS Expert	2	-	2	☎
13	Electrical Supervisor	☎	1	☎	☎
14	Electrical Technician	1	-	1	1
15	Housekeeping Staff	-	2	-	-
16	Back office Staff		2		-
17	Security Guard	2	-	2	2
18	Front Desk Executive	-	1	-	-
	<b>Total</b>	<b>8</b>	<b>14</b>	<b>8</b>	<b>6</b>

**Note:**

- Above manpower requirement table is indicative as minimum requirement for OSDC 2.0 and existing DC, bidder should have a clear prospective of the requirement of manpower to maintain the project and achieve the required SLA.
- Bidder should have their enough additional resource to meet the challenge of leave/replacement/changes for smooth delivery of services.
- General shift shall be considered as 10:00 AM to 06:00 PM excluding all state govt. holidays and national holidays.
- IT manpower (except Helpdesk Executive) & key Non IT resources mentioned in resource table must be a payroll employee of the successful bidder company.

**10.11 Compliance & Reporting Procedures**

S NO	Measurement	Definition	Measurement	Target	Penalty
1	Submission of MIS Reports and QGR reports	The Bidder shall submit the MIS reports and QGR reports Quarterly and as and when required to the OCAC/OSDC, Odisha	Quarterly	Report for the previous quarter shall be submitted within the first week of next quarter.	No Penalty
				Delay beyond the date of submission	0.01% of the QGR value for every week time delay
2.	Incident Reporting	Any failure/incident on any part of the	Quarterly	100% Critical incidents to be	No Penalty

S NO	Measurement	Definition	Measurement	Target	Penalty
		Data Centre infrastructure or its facilities shall be communicated immediately to Customer as an exceptional report giving details of downtime, if any.		reported to Customer within 1 hour with the cause, action and remedy for the incident.	
				Delay beyond an hour	1% of the QGR Payment for every hour's delay on an incremental basis.
3.	Change Management	Measurement of quality and timeliness of changes to the Data Centre facilities	Quarterly	100% of changes should follow formal change control procedures. All changes need to be approved by Customer. It should be implemented on time and as per schedule & without any disruption to business	0.1% of the QGR value for every non-compliance of Change request on an incremental basis.
4.	Scheduled Maintenance	Measures timely maintenance of the equipment installed at the Data Centre. The Bidder shall provide a detailed equipment maintenance plan on the commencement of the project.	Quarterly	100 % of scheduled maintenance should be carried out as per maintenance plan submitted by the Bidder. Any scheduled maintenance needs to be planned and intimated to Customer at least 2 working days in advance	0.1% of the QGR Payment for every non-compliance on an incremental basis
5.	Implementation of Audit Recommendations	Implementation of audit recommendations	Half-yearly	100% on time to be implemented as per timelines	0.5 % of the QGR Payment

S NO	Measurement	Definition	Measurement	Target	Penalty
		by OCAC/OSDC or its auditor which have been agreed by Bidder & Customer to be implemented.		agreed upon with Customer	for every non compliance
6.	Maintenance of Inventory	The Bidder should maintain an inventory of items that will be required on an ongoing basis for maintenance	Quarterly	100% as per the inventory log committed and maintained by Bidder.	0.1% of the QGR Payment for every non compliance

#### 10.12 Civil and Electrical Major and Minor Works

S. No	Type of work	Resolution Time	Penalty
1.	<p><b>Major</b></p> <p>Any civil/ electrical work as defined in Scope of work of this RFP</p> <p>Major Civil Work including the False Flooring, False Ceiling, Doors &amp; Locking, Partitioning, Fire Proofing of all surfaces, Furniture &amp; Fixtures and Painting to be replaced/carried out within 5 days of reporting the problem or opening of the request.</p> <p>The DCO should maintain sufficient inventory to carry out civil and electrical repairs without any disruption to operations.</p>	T= 5 days	No Penalty
		T1 = T+2 days	0.05% of the QGR for every unresolved call
		T2 = T1+2	1% of the QGR for every unresolved call
		> T2	2% of the QGR for every unresolved call

	For critical items, the resolution time shall be mutually agreed by the State and the DCO at the time of award of contract.  T shall be the agreed resolution time		
	<b>Minor</b>  Minor Civil Work including Cement Concrete Work, Masonry Work, Trench Work, Storage, Glazing and Scaffolding Work to be carried within 4 days of the reporting problem	T = 7 days	No Penalty
		T1 = T+1 days	0.05% of the QGR for every unresolved call
		T2 = T1+2	1% of the QGR for every unresolved call
		> T2	2% of the QGR for every unresolved call

(Similar table to be added for other packages)

### 10.13 SLA for existing Data Centre

The DCO shall ensure provisioning of all required services including Operation & Maintenance of all the equipment's as mentioned in the **Annexure-A (Indicative list)** for the existing SDC while monitoring the performance of the same to effectively comply with the performance levels of the new SDC i.e. OSDC 2.0. The SLA for the existing SDC located at 2<sup>nd</sup> floor, OCAC building will be same as the new SDC services except those of below mentioned parameters: -

#### A. Data Centre Uptime

S No	Measurement	Definition	Target (Quarterly)	Penalty
1.	Data Centre Uptime	Availability = {1- [(Downtime) / (Total Time in quarter - Maintenance Time in quarter)]}*100	>= 99.75%	No Penalty
			< 99.75% and >= 97.75%	For every 0.25% reduction in the uptime there will be a penalty of 0.5% QGR.
			< 97.75%	For every 0.25% reduction in the

S No	Measurement	Definition	Target (Quarterly)	Penalty
				uptime there will be a penalty of 1% of QGR.

**B. Data Centre Power Availability**

S No	Measurement	Definition	Target (Quarterly)	Penalty
2.	Data Centre Availability	Availability = $\{1 - [(Downtime) / (Total\ Time - Maintenance\ Time)]\} * 100$ Availability of Power will be measured from EMS tool.	$\geq 99.75\%$	No Penalty
			$< 99.75\%$ and $\geq 97.75\%$	For every 0.25% reduction in the uptime there will be a penalty of 0.5% QGR.
			$< 97.75\%$	For every 0.25% reduction in the uptime there will be a penalty of 1% of QGR.

**Data centre power availability = Server and Network availability.**

**C. Connectivity with SWAN and New SDC**

S No	Measurement	Definition	Target	Penalty
3.	Connectivity with SWAN and new SDC	Shall be monitored through the EMS tool from point to point.	100%	No Penalty
			<100%	For every 0.25% reduction in the uptime there will be a penalty of 0.5% QGR.

**Note:**

- All the CCTV cameras installed at existing OSDC shall be terminated and integrated with new SDC for central monitoring purpose.
- Similarly all the hardware's/Non-IT assets integrated and monitored at BMS system of existing SDC will be integrated to DCIM of new SDC for central monitoring.
- All the integration will done with prior approval for downtime.

**10.14 Important Note**

- ✓ These SLAs shall be strictly imposed and an agency shall be deployed for certifying the performance of the Agency against the target performance metrics as outlined in the tables above.
- ✓ All logs, reports and data that shall be made available for the purpose of evaluation/audit of SLA parameters/target performance metrics mentioned above for the operation and maintenance of the OSDC extension project shall be through system generated or automated monitoring tools only.
- ✓ All penalties shall be calculated on a quarterly basis unless stated otherwise. If the delays are on the part of the State, then that span of time will be excluded for the purpose of calculation of penalty.
- ✓ Cumulative penalty calculation and relative total deduction should not exceed 10% of the Total QGR value.(For O&M Phase)
- ✓ Cumulative penalty calculation and relative total deduction of three consecutive QGRs, each exceeding or equal to 10% of the QGR value on account of any reason/reasons will be deemed to be an event of default or termination.
- ✓ The ISO/IEC 27001:2015 certification should be obtained latest by end of second Quarter of the Operation phase, failing which the subsequent QGRs will be deferred till the certification is obtained and appropriate penalty as defined in SLA will be imposed.
- ✓ For the Components which are in Redundant mode or High Availability Mode or in Cluster, if one of the redundant components goes down and the services required from that particular set of components are still working/ not hampered, then the SI shall be given 24Hrs time to rectify the components, if it is still not rectified within 24Hrs, the SLA as defined above will come into existence. If in between 24hrs the other component goes down, and the entire



services required from that components are not available, the penalties as defined in the table above will come into existence from that particular point.

- ✓ If an incident has not been resolved within the stipulated time, its severity shall be escalated to the next level.
- ✓ Any virus infection and passing of malicious code shall be monitored at all levels and also user complains of virus infection shall be logged at the help desk system and collated every quarter.
- ✓ Denial of Service Attack: Non availability of any services shall be analyzed and forensic evidence shall be examined to check whether it was due to external DoS attack.
- ✓ All the measures for operational and data security and also incident handling need to be mutually agreed between the Bidder and OSDC in consultation with Consultant, based on the approvals of the composite team.
- ✓ Bidder needs to provide complete document on policy including authentication mechanisms (single/multi factor), password policies such as password length, password complexity, password expiry, account lockout policy, certificate policies, IPSEC policies etc. that will be followed in SDC, and periodic report as and when required by OSDC to track those policy in line with the policy document.
- ✓ Bidder needs to maintain an updated knowledge base of all published security vulnerabilities and virus threats for related software and microcode etc.
- ✓ Bidder needs to ensure that patches / workarounds for identified vulnerabilities are patched / blocked immediately.
- ✓ Bidder needs to respond immediately to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround / patch is made available for the same.
- ✓ Bidder shall provide a well-designed access management system, security of physical and digital assets, data and network security, backup and recovery etc.
- ✓ Operating system secured through appropriate configuration and patch updates.
- ✓ Bidder shall perform periodic reviews of domain level rights and privileges and also update the same to OSDC/OCAC.
- ✓ Bidder shall cooperate with the investigation agency when an incident has been identified.

### 10.15 SLA Change Control

It is acknowledged that this SLA may change as Customer's business needs evolve over the course of the contract period. This document also defines the following management procedures:

1. A process for negotiating changes to the SLA and methodology.
2. An issue management process for documenting and resolving difficult issues.
3. Customer and Bidder management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

Any changes to the levels of service provided during the term of this Agreement will be requested, documented and negotiated in good faith by both parties. Either party can request a change. Changes will be documented as an addendum to this SLA and, subsequently, the SLA methodology and the Contract.

### 10.16 SLA Change Process

The parties may amend this SLA by mutual agreement in accordance with terms of this contract. Changes can be proposed by either party. The Bidder can initiate an SLA review with the Customer.

Normally, the forum for negotiating SLA changes will be Customer's meetings with consultant. Unresolved issues will be addressed using the issue management process described in Clause 5 of this document.

The Bidder shall maintain and distribute current copies of the SLA document as directed by Customer. Additional copies of the current SLA will be made available at all times to authorized parties.

#### 10.17 Penalty

##### **A. Penalty Capping:**

**Note: Equipment Availability Related penalties shall be governed by the following conditions:**

1. The penalty shall be calculated on QGR as per the SLA defined.
2. The total quarterly deduction should not exceed 20% of the total applicable fee in a quarter.

##### **B. Penalty for Non-Measurable of QGR Parameters:**

The below penalty will not be included in the maximum overall QGR penalty of 20% enforced on DCO. However, in case of non-measurable of any of the two QGR parameters mentioned below, then maximum penalty of 10% or 10% plus Non Measurable Parameter Penalty which ever will be more will levied on DCO.

- a) For not measurable of Security and Incident Management SLA's. Penalty of Rs. 50,000/- would be enforced on DCO.
- b) For not measurable of IT Infrastructure related SLA's. Penalty of Rs. 50,000/- would be enforced on DCO.
- c) For not measurable of Physical Infrastructure related SLA's. Penalty of Rs. 50,000/- would be enforced on DCO.
- d) For not measurable of Major and Minor Civil/ Electrical Works SLAs. Penalty of Rs. 25,000/- would be enforced on DCO.
- e) For not measurable of Helpdesk Services. Penalty of Rs 50,000/- would be enforced on DCO.
- f) For not measurable of Compliance and Reporting SLA's. Penalty of Rs. 50,000/- would be enforced on DCO.
- g) For not measurable of Manpower Availability. Penalty of Rs 50,000/- would be enforced on DCO.

## 11. Project Management

To consider the complexity of the project, the implementation of the same requires a robust but flexible project governance and management structure. It is proposed to form a Project Monitoring Committee chaired by Competent Authority for providing overall strategy and policy guidelines with adequate members from the project stakeholders. Further, it is proposed that a Project Management Unit (PMU) shall be designed and set up for ongoing tracking of the project. The proposed PMU shall be supporting OCAC in project monitoring and management of the project. The Project Governance team should be adequately staffed and strong enough to identify the risk and suggest risk mitigation.

The Project Monitoring Committee, chaired by Competent Authority, a flexible membership will exist from the stakeholders on need basis. The committee will be supported by the Project Management Unit (PMU).

The Bidder should submit the project plan along with technical bid submission

### Indicative Reporting Mechanism

Activity	Daily	Weekly	Fortnightly	Monthly	Quarterly
Project Review Meetings by OCAC		√	√	√	√
Weekly status review meetings		√			
Daily team review meetings	√				
SLA review report		√			
Issue matrix		√			
Risk matrix			√		

### 11.1 Partial Acceptance Test (PAT)

Partial Acceptance Testing (PAT): After completion of mentioned stages of work as per timelines provided in the RFP, the System integrator shall request for Partial Acceptance Test (PAT).

Partial Acceptance Test will be conducted by the Consultant in accordance with the timelines, scope of work as mentioned in the RFP and the solution documents proposed by the System Integrator and accepted by OCAC.

The consultant will prepare and submit the report of PAT to OCAC and subject to its acceptance, it shall be deemed as completion of Partial Acceptance Test (PAT).

## 11.2 Final Acceptance Testing (FAT)

The acceptance of the Data Centre including DC site in accordance with the requirements shall be conducted. After successful testing of the features, facilities, functionalities and integrity of the commissioned devices, equipment and services by the PMU, a Final Acceptance Test (FAT) Certificate shall be issued by OCAC to the System Integrator. The date on which Final Acceptance certificate is issued shall be deemed to be the date of successful commissioning of the DC. The FAT certificate will be signed by the System Integrator, Consultant and OCAC.

The test shall include the following:

1. All civil, electrical, air conditioning works, etc., are completed as per the RFP specifications and solution documents proposed by the System Integrator and accepted by OCAC.
2. All hardware and software items must be installed at DC site as per RFP specifications and solution documents.
3. Availability of all the defined services shall be verified (by whom). The System Integrator shall be required to demonstrate all the features/facilities/functionalities as mentioned in the RFP and solution documents.
4. The PMU in consultation with OCAC shall define detailed test plan.
5. System Integrator will arrange the test equipment's required for performance verification and also provide documented test results.
6. The System Integrator shall be responsible for the security compliance of the ICT infrastructure and network before the final acceptance test.
7. All documentation as defined in the RFP should be completed before the final acceptance test.
8. The training requirements as mentioned should be completed before the final acceptance test.
9. All punch-points of Partial Acceptance Test (PAT) must be addressed and resolved before the final acceptance test.

Any delay by the System Integrator in the Final Acceptance Testing shall liable the SI for imposition of appropriate Penalties.

## 11.3 Roles and Responsibilities

### ***Role and Responsibilities – System Integrator.***

- ✓ Preparation of Design of Physical Infrastructure comprising of Civil, Electrical & Mechanical, IT and Non-IT works required to build Odisha State Data Centre 2.0. This shall also include site preparation to make it suitable for setting up a tier III Data Centre (OSDC 2.0).
- ✓ Preparation and submission of Comprehensive and Detailed Project implementation Plans and Schedules separately for each modules.
- ✓ Supply, deployment and implementation of multi-layer security, Networking, IT and Non-IT Components and other specified infrastructure at the OSDC 2.0.

- ✓ Ensure timely resolution of all errors, faults and problems related to operation of the OSDC 2.0 coordinating with the OEMs.
- ✓ Scheduled and preventative maintenance of all Equipment (active and passive) installed to run the operation of OSDC 2.0.
- ✓ Routine review of operational and other associated service availability with OCAC.
- ✓ Proper cabling and Tagging at OSDC 2.0 and should be periodically updated.
- ✓ Management, Maintenance and operations of all the OSDC 2.0 Equipment.
- ✓ Ensure compliance of Security Standards of the network and enforcing access control as per the information security policy of MeitY.
- ✓ Liaison with the Primary/Secondary Bandwidth Service Provider(s) and Internet Bandwidth provider(s) for better availability of the network as per SLA defined in this document.
- ✓ Preparation and submission of separate PAT & FAT Plans and schedules for all infrastructure, equipment's (IT and Non-IT) and services for OSDC 2.0.
- ✓ Preparation and submission of Manpower Deployment plan and schedule with list of staff to deployed under the project at various positions during different parts/stages of the project.

#### **Role and Responsibilities – OCAC**

- ✓ Provide support and suitable space for build part of OSDC 2.0 and during deployment of associated Non-IT & IT infrastructure and facilities.
- ✓ Provide the approval of design, implementation plan and schedules.
- ✓ Provide all necessary support in terms of site availability, clearances, access etc.
- ✓ Support in resolving issues and escalations with the subcontractor partner if any.

#### **Role and Responsibilities –Consultant.**

- ✓ Bid Process Management
  - Assistance in Pre-Bid meeting and resolution
  - Assistance in preparation of Corrigendum and Q&A's
  - Complete an evaluation matrix rating for each of the bidders
  - Assistance in selection of the eligible highest ranked submission(s) that have met all mandatory technical and other mandatory requirements set out in the related procurement document as per matrix
  - Assist in ensuring that the agreement between OCAC and the successful Bidder is defined formally in a signed written contract before commencement of provision of the goods, services or construction.
- ✓ Project implementation and monitoring.
  - Review the project plan and milestone prepared by the vendor and communicate deviations to OCAC

- Regular site visits during implementation phase and update status to OCAC
- Vet timelines prescribed for execution and completion of the project.
- Prepare monthly report on the progress of the supply, implementation and deviation
- Co-ordinate monthly meetings onsite with OCAC representative and bidder along with vendor (if required).
- Preparation and submission of separate PAT & FAT plans and schedules for the OSDC 2.0 infrastructure, operation and associated services.
- ✓ PAT & FAT
  - Creation of PAT test plan for all components and infrastructure
  - Identification of Test scenarios
  - Creation of PAT test cases
  - Conduct and evaluation of test cases
  - Confirmation of compliance with requirements and standards
  - Performing Final Acceptance Test of OSDC 2.0 infrastructure, operation and associated services in co-ordination with the Service Integrator.

#### **Role and Responsibilities – PMU**

- ✓ Any change-request and configuration change will be reviewed and approved by PMU.
- ✓ To monitor data from NMS system which should be configured by SI/Bidder, for auto-reporting, Dashboard, Ticket Closure System and Invoice Generation.
- ✓ Monitoring of parameters defined for System Integrator/Managed Service Provider(s) as per the signed agreement.
- ✓ Periodic Inventory monitoring and review of OSDC 2.0 equipment.
- ✓ Periodic review and monitoring of the operation & associated services and submission of report of OSDC 2.0.
- ✓ Submission of MIS reports as per the requirements of Government of Odisha/OCAC.
- ✓ Verification and Generation of Reports for monitoring implementation parameters
- ✓ Verification of Invoices submitted by the System Integrator/Managed Service Provider(s) and submission of signed reports on Correctness of the same after incorporating SLA Penalties for the purpose of release of payment by OCAC.

#### **11.4 Training**

The Bidder shall conduct training after installation and commissioning has been completed. Training shall be provided for the entire scope of work. A full-fledged training plan should be the part of the technical solution. All the training material and other associated expenses shall be borne by the SI. The training shall cover both IT and Non-IT components.

The SI shall provide a comprehensive onsite training on deployed cloud solution to the nominated member's team of OSDC.

The training course and materials should be in line / equivalent to the OEM’s syllabus for professional certifications. The training should be OEM certified instructor led and should be conducted by the respective OEMs at STPI, Bhubaneswar

All the OEMs should give hands on training on their products to the O&M team and well as OSDC team.

Sl. No.	Training Description
Non- IT Training	
1	Data Centre Design
2	Overview of Non-IT Components
3	Electrical Distribution System
4	DG System & Operation
5	UPS System & Operation
6	PAC System & Operation
7	Safety Security System & Operation
8	BMS & DCIM System & Operation
9	Data centre structured Cabling Non Intelligence solution
10	All others remaining details of OSDC
IT Training	
11	Overview of IT Components
12	Data Centre IT Architecture , Data Centre Network Design
13	Cloud Computing Environment
14	Enterprise Storage Systems Architecture
15	Enterprise Management Systems
16	Cyber Security Components
17	L1 training for network equipment’s, Servers, Operating Systems, Databases, Security equipment’s
SLA	
15	Overview of SLA Monitoring & Management
Do’s & Don’t	

Note: The above table is just minimum indicative list, type of training to be provided, however, it is required to furnish the training details along with the time period and each types of training, the target audience for the respective training and the number of people that should attend the training.

## 12 Minimum Bill of Quantity

Below mention BOQ are Indicative only, final BoQ may vary depends upon Solution proposed by Selected Bidder. Selected Bidder requested to submit detailed BoQ as per the proposed solution. Bidders must submit the complete unpriced BOQ in accordance to their solution along with the technical bid.

### 12.1 Bill of Quantity – Non- IT OSDC 2.0

**Note: This is an indicative BOQ & any other item required to make the package complete must be quoted as additional line items with quantity and price.**

**Bidders must submit the complete unpriced BOQ in accordance to their proposed solution along with the technical bid.**

S.N	Work Details	UOM	Quantity
<b>A</b>	<b>CIVIL &amp; INTERIOR WORKS:</b>		
1	Dismantling existing Wall, Doors , Window or any structure of any material	Lot	1
2	Removal of Debris from the site and disposing the same at a location as intimated by client	Lot	1
3	Brick wall with plaster	Sqr Mtr	Bidder to Propose
4	Closing of Doors, Windows if any with brick & plaster, Plywood, Gypsum etc.	Sqr Mtr	Bidder to Propose
5	Creation of Ramp with desired top finish from outside to building ground floor	Cu Mtr	Bidder to Propose
6	Creation of Toilet area with Male and female section including floor and wall tile fittings, plumbing, Electrical, doors, windows, exhausts etc. All fittings inside the toilet to be approved by OCAC before installation.	Lot	1
7	Vitrified tile flooring	Sqr Mtr	Bidder to Propose
8	Raise flooring in server hall of 300mm height	Sqr Mtr	350
9	Skirting wherever required	Sqr Mtr	Bidder to Propose
10	Gypsum partition 100 mm	Sqr Mtr	Bidder to Propose
11	Glass partition - Fire rated	Sqr Mtr	Bidder to Propose
12	Glass partition - Non fire rated	Sqr Mtr	Bidder to Propose
13	Carpet flooring	Sqr Mtr	350
14	PCC flooring	Sqr Mtr	900
15	POP and Punning	Sqr Mtr	Bidder to Propose
16	Epoxy flooring	Sqr Mtr	Bidder to Propose
17	Anti-static PVC flooring	Sqr Mtr	Bidder to Propose



18	Nitrile rubber Insulation 23 mm (minimum) under floor and roof including skirting	Sqr Mtr	850
19	PCC flooring repairing	Sqr Mtr	Bidder to Propose
20	Rolling shutter	Sqr Mtr	Bidder to Propose
21	PVC door with frame	Nos	Bidder to Propose
22	Fire rated door - for UPS rooms- minimum width 1500mm - double leaf	Nos	2
23	Fire rated door - Entry to server farm area from material lift lobby side. Minimum width 1500mm - double door	Nos	Bidder to Propose
24	Fire rated door - Entry to staging room - single leaf - minimum width 1200 mm	Nos	Bidder to Propose
25	Fire rated Glass door 1200 x 2300 single leaf	Nos	Bidder to Propose
26	Designer privacy film on glass Door	Lot	1
27	Flush door	Nos	Bidder to Propose
28	Glass doors with all accessories	Nos	Bidder to Propose
29	Modular false ceiling	Sqr Mtr	350
30	Gypsum false ceiling	Sqr Mtr	100
31	Fire rated paint	Sqr Mtr	Bidder to Propose
32	Premium Emulsion paint	Sqr Mtr	Bidder to Propose
33	Anti-Rust enamel Paint	Lot	1
34	Exterior paint	Sqr Mtr	Bidder to Propose
35	Earth pit cover	Nos	Bidder to Propose
36	Earth Excavation	Cu Mtr	Bidder to Propose
37	Earth refilling	Cu Mtr	Bidder to Propose
38	Trench cover ( RCC)	Sqr Mtr	Bidder to Propose
39	ISMB structure for ODU platform	KG	Bidder to Propose
40	Security desk	Nos	2
41	3+2 seater sofa along with tea table for waiting area near security	Nos	2
42	Centre table for waiting area	Nos	2
43	Reception table	Nos	1
44	Modular workstation desk for office area	Seat	24
45	Manager Table	Nos	3
46	Meeting room table	Nos	2
47	NOC technical desk	Nos	12
48	Bunk bed (2Tier)	Nos	1
49	Breakout area/Cafeteria Table	Nos	3

50	Breakout area/Cafeteria Chair		9
51	Staging room table	Nos	1
52	Staging room chair		3
53	NOC room Chair	Nos	12
54	Workstation chair for office	Nos	24
55	Conference table	Nos	1
56	Conference chair	Nos	10
57	Manager's chair	Nos	3
58	Manager room visitor chair	Nos	9
59	Storage Units	Nos	Bidder to Propose
60	Meeting room chair	Nos	6
61	Other chairs	Nos	4
62	Storage unit of 2 mtr height and 0.4 mtr depth, made of laminated particle board with shelves, lock and key.	Sqr Mtr	16
63	Hand operated fork lift	Nos	1
64	Paper shredder	Nos	1
65	Water filter with RO facility	Nos	2
66	Water dispenser	Nos	3
67	Shoe stand 20 pair shoe capacity	Nos	2
68	Steel Media storage 340 ltr	Nos	1
69	Creation of steps with MDF board and top surface with vinyl and anti skiding tape	Sqr Mtr	Bidder to Propose
70	DG foundation as per OEM specification	Cu Mtr	Bidder to Propose
71	DG shed	Lot	Bidder to Propose
72	Window vertical blinds	Sqr Mtr	Bidder to Propose
73	Wire Mesh partition	Sqr Mtr	Bidder to Propose
74	Fixed Iron Grill partition	Kg	Bidder to Propose
75	Key Box	Nos	1
76	Shoe Shiner ( dual shade electrically motor operated with sensor)	Nos	2
77	Dust bin (Stainless steel)	Nos	15
78	Tile puller (3 cup suction type)	Nos	3
79	Vacuum Cleaner Industrial type	Nos	2
80	Cold lock panels	Nos	Bidder to Propose
81	Emergency Exit Ramp	Mtr	Bidder to Propose
82	White board	Sqr Mtr	2
83	Pin up Notice board	Sqr Mtr	2
84	Refrigerator 300 Ltr	Nos	1
85	Tea/ Coffee Vending machine	Nos	1
<b>B</b>	<b>ELECTRICAL SYSTEM</b>		
87	HT Panel with 2 incomer and 2 outgoing and accessories	Nos	1

88	Metering panel	Nos	2
89	Dry type Transformer	Nos	2
90	Removal of existing metering panel, HT cable, HT panel, Transformer, BBT, Transformer output panel etc.	Lot	1
91	Transformer Output panel	Nos	2
92	indoor/Outdoor/Straight Through type heat shrinkable cable termination kit	Nos	Bidder to Propose as per cable schedule
93	Diesel Generator ( Data Centre continuous rated)	Nos	2
94	HSD tank and accessories	Nos	2
95	DG exhaust stack as manufacturer standard and compliance as per CPCB norms.	Mtr	Bidder to Propose
96	Fuel piping with valves and accessories.	Mtr	Bidder to Propose
97	Fuel Pump with intrinsically safe meter having feature to connect to DCIM for real time fuel consumption monitoring	Nos	Bidder to Propose
98	Cables as per cable schedule with terminations	Lot	Bidder to Propose as per cable schedule
99	UPS systems 2 x 400 KVA for Critical Load	Set	2
100	UPS systems 2 x 20 KVA for Non-Critical Load with SMF batteries including battery stand		1
101	Lithium Ion batteries for Critical load for 15 minutes back up on each UPS including battery stand..	Set	2
102	UPS input breaker with housing for critical UPS	Nos	4
103	UPS input breaker with housing for Non-critical UPS		
104	Battery bank breaker with housing	Nos	Bidder to Propose
105	DC Main LT panel 1 (MLTP 1) with all associates	Nos	1
106	DC Main LT panel 2 (MLTP 2) associates	Nos	1
107	SDC 2.0 LT panel ( SDC LPT 2) associates	Nos	2
108	Removal of existing DG Sync Panel, cable from DG to DG sync panel to LT panel	Lot	1
109	DG output panel 1 (IP 66) outdoor type	Nos	1
110	DG output panel 2 (IP 66) outdoor type	Nos	1
111	Copper Earth pit	Nos	Bidder to Propose
112	GI Earth Pit	Nos	Bidder to Propose
113	Copper earth Strip with insulation	Mtr	Bidder to Propose
114	GI Earth Strip with insulation	Mtr	Bidder to Propose
115	Distribution Board (TPN)	Nos	Bidder to Propose
116	Distribution Board (SPN)	Nos	Bidder to Propose
117	Sub mains cabling	Mtr	Bidder to Propose

118	Light and Power point Wiring	Lot	Bidder to Propose
119	Modular switch board with switches and sockets for wall	Nos	Bidder to Propose
120	Modular switch board with switches and sockets for Desk	Nos	Bidder to Propose
121	MS Conduit with accessories	Mtr	Bidder to Propose
122	PVC conduit with accessories	Mtr	Bidder to Propose
123	Flexible MS conduit	Mtr	Bidder to Propose
124	Flexible PVC conduit		
125	Smart LED lights Rectangular	Nos	Bidder to Propose
126	Smart LED light Round	Nos	Bidder to Propose
127	Smart LED Lights Square 2'x2'	Nos	Bidder to Propose
128	Smart LED lights Square 1'x1'	Nos	Bidder to Propose
129	Occupancy sensor range 6-7 meter	Nos	Bidder to Propose
130	NEMA (IEC 309) connectors with breaker	Nos	Bidder to Propose
131	BUS BAR trunk from transformer to Transformer output panel with all accessories	Mtr	Bidder to Propose
132	Track bus way ( BBT) inside Data Centre with all accessories	Mtr	Bidder to Propose
133	Tap off box with accessories for track busway system	Nos	Bidder to Propose
134	UPS output panel with K13 isolation transformer	Nos	2
135	HVAC panel	Nos	2
136	Auto transfer switch for PAC ( if required)	Nos	Bidder to Propose
137	Industrial Socket for PAC and CAC	Nos	Bidder to Propose
138	Equi-potential grid on DC below raise floor by 25x3 copper strip with insulation	Mtr	Bidder to Propose
139	Perforated cable tray (factory made galvanized). Please add items for various size	Mtr	Bidder to Propose
140	MS raceway with cover. Please add items for various size	Mtr	Bidder to Propose
141	Ladder tray. Please add items for various size	Mtr	Bidder to Propose
142	PVC raceway under PCC floor	Mtr	Bidder to Propose
143	Replacement of capacitors in existing panel and making the panel operational	Lot	1
144	Shifting capacitor panel 1 mtr backwards from its existing place for making way for new panels.	Nos	2
145	Wall fans	Nos	6
146	Ceiling Fan	Nos	3

147	Single line diagram A2 size laminated	Nos	4
148	Exhaust fan ( min 18 inch dia) with gravity damper	Nos	8
149	Clamp meter AC, DC, with clamp side suitable to fit in 240 sqr mm single core cable	Nos	2
150	Intelligent PDU for racks	Nos	180
151	Battery Impedance tester	Nos	1
152	Thermal Temperature gun	Nos	1
153	Round bottomed fire buckets-4 Nos	Set	6
154	shock treatment chart	Set	6
155	Danger boards	Nos	20
156	first aid box	Nos	2
157	Fixing of As built Single line drawing duly laminated / framed in A1 size.	Lot	1
158	cable route markers with necessary angle iron supports	Lot	1
159	Temporary lighting, temporary DB, Power Supply to all service vendor for DC construction till Go-live.	Lot	1
<b>C</b>	<b>HVAC SYSTEM</b>		
160	In-row Precision Air conditioner with all accessories	Nos	Bidder to propose
162	Front throw Precision Air conditioner for Power room - min 10 TR	Noss	4
163	Refrigerant piping with insulation and termination	Mtr	Bidder to propose
164	Dehumidifier water line piping with all accessories	Mtr	Bidder to propose
165	VRV/VRF system	HP	Bidder to propose
166	Comfort AC indoor unit	Nos	Bidder to propose
167	Refrigerant piping for VRV/VRF system with insulation	Mtr	Bidder to propose
168	Cold aisle containment with door and accessories	Sqr.Mtr	Bidder to propose
169	Sliding door on one side of hot aisle	Sqr.Mtr	Bidder to propose
170	Hot aisle containment for High density POD	Sqr.Mtr	Bidder to propose
171	Removal and closing of AHU duct at floor	Lot	1
<b>D</b>	<b>SAFETY, SECURITY, SURVEILLANCE AND MONITORING SYSTEM</b>		
172	Addressable fire alarm system with all accessories	Lot	1
173	Gas based suppression system for Server Hall	Lot	1
174	Gas passed suppression system power room	Lot	1
175	Aspiration smoke detection system	Lot	1
176	Close circuit tele vision (CCTV) NVR	Nos	1
177	PTZ Camera	Nos	3
178	Bullet fixed camera	Nos	7
179	Dome camera	Nos	42
180	55 inch Display screen	Nos	1
181	Door Access control system	Lot	1

182	Flab Barrier	Nos	2
183	Swipe barrier	Nos	1
184	Full height turnstile	Nos	1
185	Baggage scanner	Nos	1
186	Metal detector Full height	Nos	1
187	Hand held metal detector	Nos	4
188	Fire extinguisher	Nos	10
189	Water leak detection system	Lot	1
190	Rodent repellent system	Lot	1
191	Data Centre Infrastructure Monitoring system	Lot	1
192	Asset tracking system	Lot	1
193	Rack access control system	Lot	1
194	Rack humidity and temp sensor	Lot	Bidder to propose
195	Removal of fire hydrant system from server hall	Lot	1
196	Computers for Access control system	Nos	1
197	Computers for CCTV	Nos	1
198	Computer for DCIM	Nos	1
199	Data Douser	Nos	1
200	Safety Gloves, Jacket, Boot, Goggles, Fireman's axe Etc.	Set	2
201	Evacuation Chart	Nos	5
202	Signage's	Nos	30
203	Self-illumination tape	Mtr	Bidder to propose
204	Portable oxygen cylinder with mask	Nos	2
205	LED torch ( industrial type)	Nos	2
206	Portable emergency light	Nos	2
207	Visitor management system with all hardware such as Photo I card printer, Computer, camera and software etc.	Lot	1
<b>E</b>	<b>NETWORKING SYSTEM</b>		
208	Network Rack	Nos	10
209	Cat6A cable	Mtr	Bidder to Propose
210	Horizontal Cable managers	Nos	Bidder to Propose
211	Copper patch cord	Nos	Bidder to Propose
212	Patch panel	Nos	Bidder to Propose
213	MPO cassettes	Nos	Bidder to Propose
214	Blanking panel (2U)	Nos	3000
215	Cable basket min size 400mmx50mm with accessories	Mtr	200
216	Fibre Runner with accessories for all 90 racks	Lot	1
217	42U server Racks	Nos	80
218	I/O module	Nos	Bidder to Propose

219	Faceplate	Nos	Bidder to Propose
220	fibre patch cord	Nos	Bidder to Propose
221	Conduit with accessories	Lot	1
222	IP EPABX	Nos	1
223	Desk IP Phones	Nos	20
<b>F</b>	<b>CERTIFICATION &amp; HEALTH CHECK</b>		
224	Uptime Tier-III Certification	Lot	1
225	Half yearly health check	Half yearly	10
226	Liaison charges for Electrical Approvals form Electrical Inspector, Fire Department, PCB, PESO and other statutory bodies of Govt. of Orissa/India ( statutory charges if any will be paid by department/ OCAC)	Lot	1
227	ISO 9001, ISO 27001 & ISO 20000 Certification Charges	Set	1

**Note: This is an indicative BOQ & any other item required to make the package complete must be quoted as additional line items with quantity and price.**

**Bidders must submit the complete unpriced BOQ in accordance to their proposed solution along with the technical bid.**

## 12.2 BOQ of IT items

Proposed solution is for setting up cloud environment using rack servers compute

#	IT Equipment + Software + Licenses	UOM	Quantity
<b>1</b>	<b>Compute</b>		
1.1	Server Type-A (Rack Server)	Nos	18
1.2	Server Type-B (Rack Server) – Provisioned for Cloud Solution & EMS	Nos	30
<b>2</b>	<b>Network</b>		
2.1	Spine Switch	Nos	2
2.2	Leaf Switch ( Fibre)	Nos	26
2.3	Core Router	Nos	2
2.4	Management Switch -1	Nos	11
2.5	Management Switch -2	Nos	10
2.6	Leaf Switch ( Copper)	Nos	4
2.7	SDN Controller	Set	1
<b>3</b>	<b>Storage</b>		
3.1	SAN Switch	Nos	2
3.1	SAN Switch	Nos	8
3.2	Enterprise Storage	Nos	1
3.3	Tape Library Solution with Min 15 Drive	Set	1
<b>4</b>	<b>Load Balancer</b>		
4.1	Link Load Balancer	Nos	2
<b>5</b>	<b>Cyber Security</b>		

5.1	Next Generation Firewall	Nos	2
5.2	AAA	Nos	2
5.3	DDoS	Set	2
5.4	Vulnerability Assessment Solution Licenses	Nos	512
5.5	Anti- APT Solution	Nos	2
5.6	DLP Solution (Licenses)	Nos	250
<b>6 Cyber Security Software</b>			
6.1	Server Security solution (HIPS) Licences	Nos	400
6.2	Endpoint Point Security Solution Licenses	Nos	50
6.3	Datacentre Access Management (Licenses)	Nos	50
<b>7 On Premise Services (VM Based)</b>			
7.1	EMS , NMS & Helpdesk Management System	Set	1
7.2	Cloud Management & Orchestration	Set	1
7.3	Automation Software (Instance Based)	Set	1
7.4	PaaS	Set	1
<b>8 Software/License</b>			
8.1	MS Windows Server Standard Latest Edition 16 Core License	Nos	100
8.2	Red Hat Enterprise Linux 2 Core Latest Edition	Nos	30
8.3	MS SQL Enterprise Database Server Latest Edition - 32 Core	Set	1
8.4	My SQL Enterprise DB Server Latest Edition – 32 Core	Set	1
8.5	EDB post gre Enterprise Server Latest Edition – 32 Core	Set	1
8.6	Virtualization Software (For Cloud Servers)	Set	1
<b>9 Desktop / Laptop/ Printer</b>			
9.1	Desktop	Nos	35
9.2	Multifunctional Printer	Nos	2
9.3	Laptop	Nos	6



## 13 Operations and Maintenance Management

The selected bidder will provide 24x7x365 operating and maintaining services for a period of 5 years from the date of final acceptance test. The scope of the services for overall Physical and IT infrastructure management as per ITIL framework during this period shall include 24x7x365 Monitoring, Maintenance and Management of the entire Data Centre, along with providing Helpdesk services to ensure an uptime efficiency of minimum 99.982 in Odisha State Data Centre 2.0 (OSDC 2.0) and other facilities managed. This provides guarantee and accountability for the operations team, service providers and end users to meet the criteria for 24 x 7 service requirement. The goal is to achieve full uptime potential, obtain maximum leverage of the installed infrastructure or design, improve operations efficiency and realize opportunities for energy efficiency. This mainly provides the guidance and framework to drive best practices for the effective management and operations of the Odisha State Data Centre (OSDC).

- ✓ Human Resource and Planning
- ✓ Policies and Procedures
- ✓ Maintenance Management
- ✓ Operations Monitoring
- ✓ Access Management
- ✓ Training and Development
- ✓ Reports
- ✓ Documentation
- ✓ Certification
- ✓ Automation of Services

### 13.1 Commissioning of System

- i. Bidder should describe in advance the tests and details of the process that will be adopted to demonstrate the correct working of the equipment supplied both individually and as an integrated system.
- ii. System testing schedules, formats for testing and commissioning reports and dissemination mechanism for such reports shall be drawn by the Bidder in consultation with OCAC.
- iii. Commissioning of the solution shall be considered to be complete only after the following conditions have been met successfully to the satisfaction of OCAC.
  1. Successful completion of Factory Acceptance Tests and submission of necessary reports and certificates to OCAC.
  2. Delivery of all the items under the proposed bill of material at the designated locations of installation. Short shipment of goods will not be acceptable.

3. Installation and Configuration of all the components of the solutions including, but not limited to, hardware, software, devices, accessories, etc. to the satisfaction of OCAC.
4. Successful completion of Commissioning would need to be certified by OCAC and operations shall commence only after approval of OCAC.

## 13.2 Human Resource and Planning

The right number of qualified individuals organized correctly is critical to Odisha State Data Centre (OSDC) 2.0 meeting long-term performance objectives. Enough qualified in-house staff and/or vendor support must be available to perform all the maintenance activities and operate the Data Centre to provide the greatest opportunity to meet the uptime objective. All personnel working in Odisha State Data Centre (OSDC) 2.0 must have the experience and technical qualifications necessary to perform their assigned activities without impacting the Data Centre operations.

### Requirements

- Organizational Structure - this shows the structure of DC department and define which team is responsible or related to the Data Centre operations.
- DC Team Escalation Matrix – this specifies multiple user contacts to be notified in the event of critical issues or emergency.
- Staff Qualifications – this is to ensure that the team assign to handle the Data Centre are qualified, trained and has enough experience to properly manage its operations.
- RACI Matrix – this clearly states or assigns who is Responsible, Accountable, Consulted or Informed in relation to each specific tasks to be defined as per the requirement.

### Planned Resource during O & M Activity for (IT & Non-IT)

O&M Manpower Resources (Shift Wise)		Resources Detail				
SI No	IT Manpower	Qty	General Shift	1st Shift	2nd Shift	3rd Shift
1	DC Project Manager	1	√	x	x	x
2	Network & Security Administrator	1	√	x	x	x
3	Cloud & Server Administrator	1	√	x	x	x
4	EMS Specialist	1	√	x	x	x
5	Database Administrator	1	√	x	x	x
6	Storage and Backup Specialist	1	√	x	x	x
7	SIEM Analyst	1	√	x	x	x
8	Network Engineer	4	x	√	√	√

O&M Manpower Resources (Shift Wise)		Resources Detail				
Sl No	IT Manpower	Qty	General Shift	1st Shift	2nd Shift	3rd Shift
9	Server Engineer	4	x	√	√	√
10	Helpdesk Support	4	x	√	√	√
Non-IT Manpower						
11	Facility Manager	1	√	x	x	x
12	BMS Expert	4	x	√(2)	√(2)	x
12	Electrical Supervisor	1	√	x	x	x
13	Electrical Technician	4	x	√	√	√
14	Housekeeping Staff	2	√ (2)	x	x	x
15	Back Office Staff	2	√ (2)	x	x	x
16	Security Guard	8	x	√ (2)	√ (2)	√ (2)
17	Front Desk Executive	1	√	x	x	X
	<b>Total</b>	<b>42</b>	<b>14</b>	<b>8</b>	<b>8</b>	<b>6</b>

**Note:** Above manpower requirement table is indicative as minimum requirement for OSDC 2.0 and existing DC, bidder should have a clear prospective of the requirement of manpower to maintain the project and achieve the required SLA. Bidder should have their enough additional resource to meet the challenge of leave/replacement/changes and smooth delivery of services.

Key Resources & IT manpower (except Helpdesk Executive) mentioned in resource table must be a payroll employee of the successful bidder company.

### Resource Qualification and Experience

Sl No	IT Manpower	Minimum Qualification & Relevant Experience
1	DC Project Manager	B.E. / B. Tech/MCA/ Msc.IT with 10+ Years' experience including minimum 5 years' experience in Data Centre project management with PMP/Prince2 Certification. Additional MBA/PGDM will be preferable.
2	Network and Security Administrator	B.E. / B. Tech / MCA or equivalent with 10+ Years' experience including minimum 4 year experience in Data Centre network management/WAN network management with OEM Certification like CCNP/JNCP/ CCNA Security/ CompTIA Security+ or equivalent.

SI No	IT Manpower	Minimum Qualification & Relevant Experience
3	Cloud and Server Specialist / Administrator	B.E. / B. Tech/MCA or equivalent with 10+ Years' experience including minimum 5 year experience in Server management and 2 years in cloud management with OEM Certification like AWS architect/ RHCA/ VCP/ CCNA Cloud or equivalent.
4	EMS Specialist	B.E. / B. Tech/MCA or equivalent with 5+ Years' experience including minimum 2 year experience in Data Centre Operation management with any OEM Certifications like ITIL/ Application Performance Management, Infrastructure Management, eHealth, automation, Service Manager etc.
5	Database Administrator	B.E. / B. Tech/MCA or equivalent with 5+ Years' experience including minimum 2 year experience in Data Centre Operation management with OEM Certification like OCA/OCP or equivalent
6	Storage and Backup Administrator	B.E. / B. Tech/MCA or equivalent with 5+ Years' experience including minimum 2 year experience in Data Centre Operation management with OEM Certification in storage and backup area.
7	SIEM Analyst	B.E. / B. Tech with 5+ Years' experience including minimum 2 year experience in cyber security domain, cyber threat monitoring, malware analysis, with Certification like CEH/ CND/ ECSA/ CompTIA Security+
8	Network Engineer	B.E. / B. Tech or equivalent with 4+ Years' experience including minimum 2 year experience in Data Centre/ WAN /LAN with OEM Certification like CCNA/CCNP/JNCA
9	Server Engineer	B.E. / B. Tech/MCA or equivalent with 4+ Years' experience including minimum 2 year experience in Server management with OEM Certification like MCP/MCSE/RHCE or equivalent
10	Helpdesk Desk	BCA/BSc.IT or any Graduate with 2+ Years' relevant experience. Preferable IT knowledge for LAN/WAN/Cloud etc.

SI No	Non IT Manpower	Minimum Qualification & Relevant Experience
1	Facility Manager	B.E. /B. Tech in Electrical or equivalent with 10 Years' experience including minimum 4-year experience in Data Centre Non-IT Operation Management of Non-IT services.
2	BMS Expert	Diploma in Electrical/ EEE or higher qualification with 8+ years' of experience including minimum 3-years' experience in Data Centre BMS environment.
3	Electrical Supervisor	Diploma in Electrical with 8 Years' experience including minimum 3-year experience in HT/LT Installation/ Maintenance.
4	Electrical Technician	ITI in electrical/EEE with 2 Years' relevant experience

SI No	Non IT Manpower	Minimum Qualification & Relevant Experience
5	House Keeping	With relevant experience of 6 months or more.
6	Back Office	Matriculation or higher with relevant experience of 1 year.
7	Security Guard	With relevant experience of 3 years or more.
8	Front desk Executive	Graduate with good communication skill and PGDCA or higher with 1 Years' of relevant experience.

**Note:**

- All the above mentioned employee's Qualifications and Certifications will be verified by OCAC/Composite Team after award of the contract. The same will be verified by Consultant/PMU (assigned) on time to time basis during the Operation and Maintenance phase of bidder.
- Upon finding any deficiency in any of the profile parameter, may reject any of the manpower by giving 15 days' time, which the bidder has to replace the resource within the time frame.

**13.3 Policies and Procedures**

An effective Odisha State Data Centre (OSDC) 2.0 management strategy includes policies and procedures that needs to be documented and enforced to ensure that they are understood and followed as inconsistencies in the performance can lead to service interruptions or downtime.

**Requirements**

- Data Centre User Manual – This includes all information that is critical to run the Data Centre from construction phase to operation.
- Data Centre Instructions – This are set of rules inside the Data Centre that prevents any risk to Data Centre operations.
- Emergency / Crisis Management Plan – this is to ensure control and management inside the Data Centre during an emergency or abnormal situations.
- SOP's – Set of instructions or guide to operate DC configurations on normal conditions
- Health & Safety Procedures – Set of HSE guidelines specifically for the Data Centre to prevent accidents or harm to the DC team or visitors.
- Change Management Procedures – this is to review and approve the proposed changes and evaluate the risk that comes with it.
- Access Procedures - this access guideline specifies the criteria for granting access to specific individuals or groups, and the different levels of access allowed.

- Maintenance Procedures – this specifies how a maintenance procedure is scheduled and performed.

### 13.4 Maintenance Management

An effective maintenance program is necessary to keep equipment in an optimum condition, minimize failures and prevent downtime. This includes preventive and predictive maintenance, strong vendor support, failure analysis, life cycle tracking and documentation. Any level of vendor support to maintain infrastructure should have a corresponding list of qualified vendors with formal contracts specifying the scope of work, call-in process, qualifications, and response times to ensure the level of service required meets the uptime objectives. Housekeeping is also an equally important aspect of maintenance to keep combustibles and contaminants out of the Data Centre and technical rooms. For the purpose of proper upkeep of equipment's installed at Odisha State Data Centre (OSDC) 2.0, there is a need to study OEM documents:

#### **Requirements**

- List of Equipment – this includes Generator, UPS, HT Panel, LT Panel cooling, Fire Alarm & Suppression, Access control & CCTV and related sensors. It is an indicative list not an exhaustive one.
- Specialized Vendor Details – This contains the details of the vendor(s) assigned to maintain DC equipment. Technician information, qualifications and certifications should be available.
- Service Level Agreements – Should clearly define the Response Time and Conditions to match our requirement as well as OEM recommendations.
- Planned Preventive Maintenance (PPM) – PPM schedule should be fixed for the entire period of contract. So we can plan other activities accordingly without conflict.
- Sequence of Operation – This shows the operation of any equipment with redundant functionality in case of a primary source failure. Example: UPS, Generator, Etc.
- Escalation Matrix or Emergency Call-out Matrix – This allows to clearly identify the response team responsible for any equipment failure
- Service Evaluation – This is to evaluate the assigned team and request for changes if required. This will increase the quality to the support from the service team.
- Methodology and Risk Assessment – This is to provide information on how the maintenance will be performed and the risk that comes with it. This is required for all maintenance activities – may it be major or minor.
- Housekeeping Schedule – This can either be planned or on-call but otherwise required. Housekeeping Team will be supervised at all times.
- Critical Spare Parts - These are list of spare parts to be made available on site to sustain operation of DC critical equipment.

- End-of-life study – This is to indicate that the product is in the end of its useful life and the vendor stops marketing, selling, or sustaining it.
- Life Cycle study – This will enable the team to know when the equipment has reached its peak performance and will be subject to replacement.
- Predictive Maintenance – This will allow the team to alter PPM schedule to match the equipment maintenance as required.
- Anticipation and Forecasting – This is essential for laying out plans to sustain or improve the Data Centre services.

### 13.5 Operations & Maintenance Monitoring

The O& M monitoring should continuously observe at the network level for the ability to look at all assets, physical and virtual, that reside on the LAN, even those that are offline, and all inter-connections between them. This monitoring should be done on a continuous basis and should be capable of monitoring dynamic network fabrics. This is should also include monitoring for missing patches or application or configuration changes that can introduce vulnerabilities that can be exploited.

#### **Requirements**

- Physical or Visual Inspection – This should be on daily basis at random times. Daily inspection should be routine work for the Data Centre managers. This involves visual checking of the electrical devices, cooling equipment, UPS, sensors, lighting, etc.
- Online / Remote monitoring – This type of monitoring is applied to all Data Centre components connected to the network (DCIM) and also to the BMS alerts. This shows actual information received from sensors, smart devices, etc.
- Critical Alerts – There should be an automated system capable of sending alerts or notification through Email or SMS to all Data Centre managers for any critical system failure that requires immediate action.

### 13.6 Access Management

This access guideline specifies the criteria for granting Odisha State Data Centre 2.0 (OSDC 2.0) access to specific individuals or groups, and the different levels of access allowed. These are composed of instructions and policies to restrict and prevent unauthorized and unqualified access that may cause any type of risk to our operation.

#### **Requirements**

- Permit to Access (PTA) – This provides access to the Data Centre strictly for inspection or survey purposes only. Any type of work or configuration will not be allowed.



- Permanent Access – given to authorized or qualified Data Centre managers or operations team only.
- Temporary Access – also called visitor access. This is given to individuals authorized to access the Data Centre for a period of time, with proper approval from OCAC or authorized person.
- Permit to Work (PTW) – This allows an individual to do work such a configuration, updates, shutdown, patching, maintenance etc. This also applies to DC maintenance vendors.
- Permit to Modify Equipment (PTME) – This allows an individual to add, remove or replace any equipment from the Data Centre, with proper approval from OCAC or authorized person.
- No Objection Certificates (NOC) – This is to allow any new requirement or projects directly impacting Data Centre operations.
- Change Request Forms (CR) – This is required for any major modification or change request on the existing setup of the Data Centre. This also covers revoking access permissions to existing permanent users.

### 13.7 Training and Development

Proper training and induction ensures that the team understands the policies, procedures, and unique requirements for working inside the Data Centre. This is essential in avoiding unplanned outages and ensuring proper response to both anticipated and unplanned events.

#### **Requirements**

- Data Centre Induction – This is having the team familiarize with the existing configuration of the Data Centre and to follow the guidelines for operation.
- Data Centre Trainings – All DC operations team should have the basic and effective knowledge on how the facility operates as per the implemented design. This involves network connection, power, cooling and support.
- Bidder shall provide all necessary training to OCAC officials and authorised team members for the purpose of successful functioning of the Data Centre operation and management.

### 13.8 Documentation

These are set of references or records provided on paper or on digital media. These documents act as the store of collective organizational and operational knowledge regarding the processes and can be accessed by anyone in times of need. All these documents should be latest, updated, protected and available.

#### **Requirements**

- Asset list – list of equipment installed for Data Centre operations.
- As-built drawings – final approved layouts as installed before activation. This is used as basis and includes civil, electrical, IT, Non-IT, and passive components.

- Licenses – licenses for all IT, Non-IT, applications, databases and passive components (wherever applicable) should be made available for support and service.
- Operation manuals – used as reference for the equipment functions.
- Procedure manuals – used as reference for the specified OEM procedures.
- Data Sheets – reference for equipment specification.
- Equipment Set Points – reference for equipment configuration.
- Testing and Commissioning – verifies proper operations of systems via documented testing procedures and establishes performance criteria in line with OEM standards.
- Warranty Certification – an effective warranty management program secures operational stability through knowing the limits and exceptions of the product as per OEM. This includes all electrical, IT, Non-IT, and passive components (wherever applicable) and should be made available for support and service.

### 13.9 Reporting

This is to communicate the compiled information as outcome of any activity related to the Data Centre operations. It is important that these documents are accurate, objective and complete according to its purpose as this is the only relevant factor used for referencing.

- a. Data Centre Activity Report – This includes total number of PTA (Permit to access), PTW (Permit to Work), NOC and CR (Change Request) can be monitored monthly, quarterly and annually.
- b. PM (Preventive maintenance Reports) – This should be submitted monthly or as per OEM. This ensures proper maintenance has been done.
- c. Incident Report – It is required to monitor every incident to prevent recurrence.
- d. KPI Report – This is to monitor all targeted activities. Can be monitored monthly, quarterly and annually.
- e. The reports supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds (MOTT) and the other that monitors service transaction response time.
- f. The system must provide a historical reporting facility that will allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.
- g. The system should provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity should be provided out of the box.
- h. The system should display option on Services, Customer, SLA's, SLA templates. The customer definition option should allow to associate a service or an SLA with a customer.

### 13.10 Monthly reports

Consolidated component-wise ICT infrastructure availability and resource utilization report as mentioned bellow has to be submitted to all the stockholders involved in the project in hardcopy as well as in softcopy.

1. Component wise IT infrastructure availability and resource utilization.
2. Consolidated SLA / non-conformance report.
3. Summary of issues / complaints logged at the Technical Support desk
4. Summary of resolved, unresolved and escalated issues / complaints
5. Issues / Complaints Analysis report for virus calls, call trend, call history, etc.
6. Summary of systems rebooted.
7. Log of backup and restoration undertaken
8. Summary of issues / complaints logged with the OEMs.
9. Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.
10. Summary of component wise Data Centre uptime.
11. Summary of changes in the Data Centre.
12. Log of preventive / scheduled maintenance undertaken
13. Log of break-fix maintenance undertaken
14. Summary of attendance of bidder's staff at the Data Centre.
15. Inventory of spare parts in the Data Centre.

### 13.8.2 Quarterly reports

Consolidated as well as detail component-wise ICT infrastructure availability, bandwidth utilization, resource utilization and manpower availability report as mentioned bellow has to be submitted to all the stockholders involved in the project in hardcopy as well as in softcopy.

1. Component wise IT infrastructure availability and resource utilization.
2. Consolidated SLA / (non)-conformance report.
3. Summary of component wise Data Centre uptime.
4. Summary of changes in the Data Centre.
5. Log of preventive / scheduled maintenance undertaken
6. Log of break-fix maintenance undertaken
7. Details of attendance of manpower availability at the Data Centre.

### 13.8.3 Half-Yearly reports

Consolidated component-wise ICT infrastructure availability and resource utilization report as mentioned below has to be submitted to all the stockholders involved in the project in softcopy.

1. Data Centre Security Audit Report
2. IT infrastructure Upgrade / Obsolescence Report.
3. Consolidated component-wise ICT infrastructure availability and resource utilization report to be submitted to all the stockholders involved in the project in hardcopy.

### 13.8.4 MIS reports and deliverables

The Bidder shall be required to submit the reports as specified hereunder on a regular basis in a format decided by OCAC. The following is only an indicative list of MIS reports which should be in conjunction to the reporting features highlighted in RFP. The bidder should submit reports to all the stockholders involved in the project and hardcopy may have to be submitted as when required or asked by OCAC.

### 13.8.5 Incident Reporting

A. Software license violations:

1. OCAC shall get the IT infrastructure solution audited by a third-party on yearly basis. The third party shall undertake the audit of the entire IT infrastructure solution. The audit shall ensure installation of proper versions of software including, but not limited to, Firmware, OS patches, etc.
2. The audit report shall make recommendations to OCAC regarding issues including but not limited to upgrade of infrastructure components, reallocation of unused infrastructure components, etc.
3. The audit shall also cover obsolescence of the IT infrastructure as per the policy defined by the bidder in discussion with OCAC. The audit report shall provide details of the infrastructure components that are due for obsolescence and provide recommendations for upgrade / refresh of infrastructure components and plan for disposal of obsolete infrastructure components.
4. OCAC may also get a half-yearly security audit done by a third-party for the security practices, implementation of security policy and vulnerability assessment at the Data Centre. The security audit report shall rate the security implementation in three grades viz. Satisfactory, Requires Improvement and Unsatisfactory.
5. Bidder shall provide necessary support and co-operation for these audits.
6. Bidder shall implement all the audit recommendations in time as per the service levels defined in Section Service Level Agreement.

B. Documentation.

1. Bidder shall be required to submit documentation in the format, media and number of copies as decided mutually with OCAC. The documentation shall be kept updated throughout the contract period with appropriate change management procedures and version control. It is advisable to follow international standards and best practices like ISO standards while creating the documentation.
2. Bidder shall provide documentation, which follows the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the project undergoes various stages of implementation. Indicative list of documents include:
  - i. Project Commencement: Project Plan in MS Project giving out micro level activities with milestones & deadlines
  - ii. Delivery of Material: Original Manuals from OEMs.
  - iii. Training: Training Material will be provided which will include the presentations used for trainings and also the required relevant documents for the topics being covered.
  - iv. Process Documentation: Bidder shall be responsible for preparing process documentation related to the operation and maintenance of each and every IT component of the SDC. The prepared process document shall be formally signed off by OCAC before completion of final acceptance test.
  - v. Bidder shall document all the installation and commissioning procedures and provide the same to OCAC within one week of the commissioning of the SDC.
  - vi. Manuals for configuring of switches, firewall, IPS etc shall be provided by the Bidder.
  - vii. Bidder shall be responsible for documenting configuration of all devices and keeping back up of all configuration files, so as to enable quick recovery in case of failure of devices.
  - viii. Bidder shall submit the report on best security practices & further improvement & enhancement of the SDC to OCAC.
  - ix. SDC, being a property of OCAC, it reserves the right to verify the process and documentation submitted, at any given point of time
  - x. Bidder shall be responsible for creation and maintenance of all the documentation including but not limited to configuration documents, network diagram, Data Centre operation manual, system administration manual, security administration manual, password management manual, etc. The servicing manual should cover all the procedures and information necessary for the diagnosis and repair of faulty units or components of every type.
  - xi. Bidder shall get all these documents approved by OCAC.

- xii. Bidder shall be also responsible for maintenance and updation of all the policy documents including but not limited to security policy, backup policy, archival policy, backup policy, anti-virus policy, etc.
- xiii. Bidder shall make changes to the documents as and when there is change in the IT infrastructure components or policies or as and when required by OCAC.
- xiv. Bidder should maintain a library of various artefacts including, but not limited to, documents, manuals, knowledge bases, CD / DVDs, etc. pertaining to all the components supplied by various OEMs. Bidder should keep a track of all the artefacts and manage the issue and return of the artefacts into the library.
- xv. All the documents would be solely owned by OCAC.

C. Training – Information Security & BCP:

1. Technical Training before Go-Live:

- i. The bidder should also provide technical training on all equipment to officials as designated by OCAC.
- ii. The contents of such training would need to be documented and made available to all the attendees.
- iii. The exact duration, schedule and coverage of trainings shall be discussed with the Bidder at the time of contract.

2. Operational Training after Go-Live:

- i. Bidder shall impart operational training to all the primarily the designated resources of OCAC. This training should cover a session on Security Awareness, practices and operations for the information security and BCP components installed at the Data Centre.
- ii. The standard contents of such training should be documented and made available to all the team members of OCAC who are involved under OSDC 2.0 project

**13.8.6 Performance - Monitoring, Management and Reporting**

The proposed performance management system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The proposed performance management system must integrate network, server & database performance reporting information and alarms in a single console in order to provide a unified reporting interface.

**13.8.7 Constitution of the Team**

- 1. The Bidder shall provision for adequate onsite support to provide 24x7x365 onsite operations and maintenance services to OCAC as defined in the scope of work.

2. Bidder shall provide adequate number of administrators, each responsible for its respective specific role at the SDC. The bidder must provide clear definition of the role and responsibility of each manpower resource as part of the Technical Bid in the format specified in Contents of the Bid.
3. Onsite resources will follow six working days per week cycle, and will be entitled for all national holidays. In required resources would be called on Holiday/odd hours, in such case they will be entitled for compensatory leaves.
4. All the critical (L2 & above) onsite resources deployed at SDC have to be on Bidder's payroll.
5. Onsite resources for Network, Security and technical support will work in shifts to provide 24x7x365 onsite operations and maintenance services to SDC.
6. All the concerned onsite staff shall log an attendance on a daily basis. Bidder shall maintain a database of attendance of his staff at the SDC. The attendance database should have facility to track attendance and draw out MIS reports as desired by OCAC. Bidder shall submit the attendance records in a format and as per schedule desired by OCAC.
7. Bidder should ensure that all the personnel identified for this project have high level of integrity. Bidder should undertake necessary due diligence to ensure that the personnel have high standard of trustworthiness. Bidder should obtain an undertaking from each of the personnel assigned and the same should be submitted to OCAC as and when demanded by OCAC.
8. Bidder shall be responsible for any mishaps or security breaches that happen due to bidder's personnel / personnel appointed by bidder for execution of services.
9. A Project In-charge should be appointed on a full-time basis. The Project In-charge shall be responsible for the overall project and shall be a single point of contact for OCAC.
10. Bidder should estimate and propose the personnel required during the Installation, Commissioning and Maintenance phase and provide the estimation as part of the Technical Bid in the format specified in Contents of the Bid.
11. The following clause defines the skill sets and qualification requirement for Project In-Charge.
12. Project In-charge
  - i. Should be deployed at the Data Centre site on a full-time basis.
  - ii. Should be responsible for the overall contract performance and should not serve in any other capacity under this contract.
  - iii. Should be responsible for organizing, planning, directing, and coordinating the overall program effort and managing the team.

- iv. Should have extensive experience and proven expertise in managing infrastructure project of similar type and complexity.
- v. Should have a thorough understanding and knowledge of the principles and methodologies associated with program management, vendor management, quality assurance metrics and techniques, and configuration management tools.
- vi. Should have a graduation degree in Engineering with PMP certification.
- vii. Should have an IT experience of 10 years with minimum 5 years of relevant experience in Data Centre with PMP /Prince2 Certification and complying to Eligibility criteria mentioned in this RFP.
- viii. ITIL certification would be preferable.

#### 13.8.9 O & M Roles and Responsibilities

##### Responsibilities of the Bidder:

1. Bidder shall prepare and then seek approval from OCAC on all the IT infrastructure solution architecture, diagrams and plans before commencement of installation.
2. Bidder shall follow Change Management Procedures, Information Security Policies as suggested by OCAC.
3. Bidder shall ensure proper handover/ takeover of documents & other relevant materials in the event of change in personnel.
4. Bidder shall share and review all internal documents / reports used to monitor & execute the project with OCAC as and when desired.
5. Bidder shall proactively interact with other vendors / third parties / OEMs to ensure that the equipment is upgraded and maintained at a periodic interval. OCAC would only pay the services charges applicable for operations and maintenance of the Data Centre.
6. Bidder would manage all aspects of Vendor management.

##### Responsibilities of OCAC:

1. OCAC shall provide approvals & sign-offs to the deliverables within the stipulated time period.
2. OCAC shall direct and monitor the activities performed by the Bidder as per the RFP Document and in turn validate the service levels attained as per the SLA document.

#### 13.8.10 Certification

There are various operational standards to select from. International Standard Organization (ISO) has provided these standards that guide day-to-day processes and procedures once the Data Centre is built. All these documents should be latest, updated, protected and available.

##### **Requirements**

- ISO 9001
- ISO 20000
- ISO 27001



- ISO 27017

#### 13.8.11 Automation of Services

Odisha State Data Centre (OSDC) 2.0 services should be automated or through the building management system & incident management system to request and approve of the following:

- Permit to Access
- Permit to Work
- Permit to Modify Equipment
- NOC
- Change Request
- All DC alerts related to critical equipment should be recorded and alerted through SMS or Email to all concerned.

#### 13.11 Handing Over Taking over (HOTO Plan)

Selected SI should understand, analyse and examine the current state of the existing SDC on AS-IS basis in discussion with and knowledge transfer from the current DCO, Project Consultants, Composite team, OCAC and other stakeholders. The process of handover has to be seamless without any disruptions to the existing services as per a HOTO plan to be mutually agreed by all stake holders along with the selected SI and current DCO. The complete handing over taking over (HOTO) activity will be done by the existing operator to the new operator as a transition sub-project.

The transition period will be maximum of 90 days or less as per the agreed aforementioned HOTO plan. The HOTO activities should be jointly identified by the selected MSI, current DCO and OCAC. There will be a team comprising of new and existing SI (service provider) for completion of the identified activities under the HOTO plan. The selected SI will depute a Transition Team for OSDC to take over the identified activities (knowledge transfer, asset transfer, operations transfer, etc.).

Selected SI should perform site survey to verify the inventory details provided by current DCO and Composite Team with the actual on-site inventory. A report on site survey should be submitted to OCAC highlighting the discrepancies in the form of GAP report. Site survey should be done for the entire OSDC, inclusive of active as well as passive elements. The site survey report detailing on all IT and non-IT equipment should enlist the details about the assets and their working status (working, not working, end of life, etc.), status of software's (like; license expired, license expiry date, license valid till date etc.).

Selected SI should undertake takeover of equipment and operations from the current DCO with due diligence. The overall facilitation and moderation of the HOTO would be the responsibility of OCAC.

The current DCO will provide the following to the selected SI:

- Current scope of work
- A detailed documentation of the transfer process that could be used in conjunction with a selected SI including details to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
- Proper communication matrix with such like DCO, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on DC project's operation as a result of undertaking the transfer.
- Entitlement for assets to be used by selected SI for the duration of the exit management period.
- Information relating to the current services rendered and performance data relating to the performance of the services; Documentation relating to Intellectual Property Rights; any other project data and confidential information; all current and updated SDC Project data as is reasonably required for purposes of the SDC Project or for transitioning of the services to selected MSI in a readily available format.
- All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable the Client and its nominated agencies, or its selected SI to carry out due diligence in order to transition the provision of the services to Client or its nominated agencies, or its replacement Selected SI (as the case may be).

The takeover of OSDC should include:

- Process, Policies & Guidelines;
- Inventory & Asset details (IT, Non-IT and Utilities);
- IT & Non-IT Architectures (layouts & diagrams)
- Configuration & Back Up file of each device;
- AMC documents , Preventive Maintenance documents;
- Standard Operating Procedures;
- ISO compliance documents;
- Non-disclosure affidavits with concerned OEMs and vendors;
- License status (Validity, expiry details);
- Manpower deployment plan;
- Previous Audit Reports including QGR calculations;
- Capacity Management plan document;
- Operations, Maintenance and Management of SDC responsibilities;

- Security & Data Privacy reports;
- MIS reports

Selected SI would be provided with the detailed exit management plan submitted by the Existing SI to align their activities for HOTO and ensure completion of same within 90 days or less. The existing DCO has to provide shadow support for a period of 10 working days during operational takeover of the SDC.

The deliverable for completion of this phase would be the sign off of HOTO Report from OCAC or its nominated agency and submission of AMC documents of existing IT/Non IT equipment/software/license as per RFP requirement to OCAC.

## 14 Proforma and Schedules

### 14.1 Proforma 1: Proposal Covering Letter

#### **PROPOSAL COVERING LETTER:**

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Sir/Madam,

Ref: Request for Proposal (RFP): Selection of System Integrator for “Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar”

Have examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide best of quality goods and professional services as required and outlined in the RFP for the Selection of System Integrator for Design, Build, Commission and O&M of Odisha State Data Centre 2.0 (OSDC 2.0) to meet such requirements and provide such services as required are set out in the RFP.

We attach hereto the technical response as required by the RFP, which constitutes our proposal. We undertake that, if our proposal is accepted, to adhere to the Project Timeline and Service Levels given in the RFP for various activities.

If our proposal is accepted, we will obtain a performance bank guarantee in the given format in the RFP document issued by a Scheduled Commercial Bank in India, acceptable to OCAC, for a sum equivalent to 10% of the total price as quoted in our financial proposal for the due performance of the contract.

We agree for unconditional acceptance of all the terms and conditions set out in the RFP document and also agree to abide by this RFP response for a period of 180 days from the bid opening date and it shall remain binding upon us with full force and virtue, until within this period a formal contract is prepared and executed, this RFP response, together with your

written acceptance thereof in your notification of award, shall constitute a binding contract between us and OCAC.

We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to OCAC is true, accurate, and complete. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead OCAC as to any material fact.

We agree that you are not bound to accept the lowest or any RFP response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products / services specified in the RFP response.

It is hereby confirmed that we are entitled to act on behalf of our corporation/ company/ firm / organization and empowered to sign this document as well as such relevant documents, which may be required in this connection.

Dated this \_\_\_\_\_ Day of 2020

(Signature)

(In the capacity of)

Having the Power of Attorney & duly authorized to sign the RFP Response for and on behalf of:

(Name and Address of Company)

Seal/Stamp of Bidder

Witness Signature:

Witness Name:

Witness Address:

**CERTIFICATE AS TO AUTHORISED SIGNATORIES**

I, certify that I am ..... of the ....., and that ..... who signed the above Bid is authorized to bind the corporation by authority of its governing body.

## 14.2 Proforma 2: Declaration of Acceptance of Terms & Conditions of RFP

### **DECLARATION OF ACCEPTANCE OF TERMS & CONDITIONS CONTAINED IN THE RFP**

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Sir/Madam,

I have carefully gone through the Terms & Conditions contained in the RFP Document [OCAC/\_\_\_\_\_/\_\_\_] regarding RFP for Selection of System Integrator “Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar”

I declare that all the provisions of this RFP document read along with the proposal submitted by my Company. I certify that I am an authorized signatory of my company and therefore, competent to make this declaration. I further certify that, interpretation made by OCAC technical committee is the final and binding on me.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

### 14.3 Proforma 3: Undertaking on Total Responsibility

#### **Undertaking of Total Responsibility**

(On the Bidder's Letterhead)

RFP Ref. No. OCAC/\_\_\_\_\_/\_\_\_\_

Date:

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Dear Sir,

Sub: Undertaking on Total Responsibility for Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar.

This is to certify that we undertake total responsibility for the successful and defect free operation of the proposed Project, as per the requirements and terms and condition of the RFP for Selection of System Integrator for "Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar"

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

#### 14.4 Proforma 4: Format of Technical Proposal Document

RFP Ref. No.: OCAC/\_\_\_\_\_/\_\_\_\_

Date:

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Subject: Submission of Technical proposal for "Selection of System Integrator for Design, Build, Installation, Commission, Integration and O&M of Odisha State Data Centre 2.0 (OSDC 2.0)".

Dear Sir/Madam,

We, the undersigned, offer to provide Systems Implementation solutions to OCAC Ltd on <Name of the Systems Implementation engagement> with your Request for Proposal dated <insert date> and our Proposal. We are hereby submitting our Proposal, which includes this Technical bid and the Financial Bid separately.

We hereby declare that all the information and statements made in this Technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

We undertake, if our Proposal is accepted, to initiate the Implementation services related to the assignment not later than the date indicated in Data sheet.

We agree to abide by all the terms and conditions of the RFP document. We would hold the terms of our bid valid for 180 days as stipulated in the RFP document.

We hereby declare that we are not insolvent, in receivership, bankrupt or being wound up, our affairs are not being administered by a court or a judicial officer, our business activities have not been suspended and we are not the subject of legal proceedings for any of the foregoing.

We understand you are not bound to accept any Proposal you receive.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:



## 14.5 Proforma 5: Forwarding Letter for Earnest Money Deposit

### Forwarding Letter for Earnest Money Deposit

From (Name & complete address of the bidder) _____ _____ _____ _____	To General Manager (Admin) Odisha Computer Application Centre, N1/ 7D, Acharya Vihar Square, Near Planetarium, P.O. – RRL, Bhubaneswar, Odisha, Pin-751013
--	--

Dear Sir/Madam,

**Subject: EMD submission for the RFP "Selection of System Integrator for Design, Build, Commission and O&M of Odisha State Data Centre 2.0 (OSDC 2.0) OCAC tower, Bhubaneswar"**

**Reference: RFP number <OCAC/\_\_\_\_/\_\_\_\_>**

**Dated <\_\_/\_\_\_\_/\_\_\_\_>**

We, M/s <\_\_\_\_\_>, having carefully read and examined in detail the RFP document for ""Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar"" at OCAC Tower, Bhubaneswar, published by OCAC hereby submit EMD of Rs. <\_\_\_\_\_>/- (Rupees <\_\_\_\_\_> Only) in the form of Bank Guarantee. The details are as under:

Name of Issuing Bank :

Bank Guarantee number :

Amount :

Dated :

We M/s \_\_\_\_\_ have read and understood the clauses of RFP document towards forfeiture of EMD.

Thanking you,  
Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

Encl: - Copy of Earnest Money Deposit

#### 14.6 Proforma 6: Format for furnishing Earnest Money Deposit

Whereas \_\_\_\_\_ (hereinafter called the “tenderer”) has submitted their offer dated \_\_\_\_\_ for Selection of System Integrator for “Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar” (OSDC 2.0) hereinafter called the “RFP”) against the purchaser’s RFP enquiry No. OCAC/\_\_\_\_\_/\_\_\_\_\_ KNOW ALL MEN by these presents that We \_\_\_\_\_ < Bank Name> of \_\_\_\_\_ having our registered office at \_\_\_\_\_ are bound unto \_\_\_\_\_ (hereinafter called the “Purchaser”) in the sum of \_\_\_\_\_ for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents.

Sealed with the Common Seal of the said Bank this \_\_\_\_ day of \_\_\_\_\_, 2020.

#### **THE CONDITIONS OF THIS OBLIGATION ARE:**

- (1) If the tenderer withdraws or amends, impairs or derogates from the RFP in any respect within the period of validity of this RFP.
- (2) If the tenderer having been notified of the acceptance of his RFP by the purchaser during the period of its validity:-
  - a. If the tenderer fails to furnish the Performance Security for the due performance of the contract.
  - b. Fails or refuses to accept/execute the contract.

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 180 days from the last date of RFP submission date/ RFP validity date and any demand in respect thereof should reach the Bank not later than the above date.

\_\_\_\_\_  
(Signature of the authorized officer of the Bank)

\_\_\_\_\_  
Name and designation of the officer

\_\_\_\_\_  
Seal, name & address of the Bank and address of the Branch

## 14.7 Proforma 7: Company Profile of Bidder

**Company Profile of the Bidder**

Requirements	Details	Remarks
Name of the Company/Firm		
Date of Incorporation (Registration Number & Registering Authority)		
GST and PAN No.		
Legal Status of the Company in India	Public Ltd Company/ Private / Partnership Firm	
& Nature of Business in India		
Address of the Registered Head Office in India		
Date of Commencement of Business		
Address of the office in Odisha (if any)		
Active ISO/ SEI CMMI Level status ( Enclosed Certificate)		
Details of the Contact Person	Name: Designation: E-mail id: Phone& Fax number:	
Details of the Contact Person to whom all references shall be made regarding this RFP	Name: Designation: E-mail id: Phone& Fax number:	
Web-Site & -mail ID for any grievance		

(Seal &amp; Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

## 14.8 Proforma 8: Declaration regarding Clean Track Record

### **DECLARATION REGARDING CLEAN TRACK RECORD**

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Sir/Madam,

I have carefully gone through the Terms & Conditions contained in the RFP Document [OCAC/\_\_\_\_/\_\_\_] regarding RFP for Selection of System Integrator for "Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar".

I hereby declare that my company has not been debarred / blacklisted by any Government / Semi-Government organizations of Central Govt./ State Govt. / PSUs. I further certify that I am competent authority in my company has authorized me to make this declaration.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

## 14.9 Proforma 9: Undertaking on litigation

### **Undertaking on litigation(s)**

This is to certify that << COMPANY NAME >> is not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this RFP.

Company Secretary / Authorized Signatory

Name of Signatory:

Bidder Company Name:

Date:

Place:

#### 14.10 Proforma 10: Undertaking on Not Being Black-Listed

##### **Undertaking on Not Being Black-Listed**

This is to certify that << COMPANY NAME >> is not blacklisted by the Government of Odisha or any of its agencies for any reasons whatsoever and not blacklisted by Central / any other State/UT Government or its agencies for indulging in corrupt or fraudulent practices or for indulging in unfair trade practices and not backed out from executing the work after award of the work as on the RFP submission date.

Company Secretary / Authorized Signatory

Name of Signatory:

Bidder Company Name:

Date:

Place:

## 14.11 Proforma 11: Undertaking of Service Level Compliance

### **Undertaking of Service Level Compliance** (On the Bidder's Letterhead)

RFP Ref. No.: OCAC/\_\_\_\_\_/\_\_\_

Date:

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Dear Sir/Madam,

Sub: Undertaking on Service Level Compliance

1. I/We as Implementing Agency do hereby undertake that we shall monitor, maintain, and comply with the service levels stated in the RFP to provide quality service to OCAC.
2. However, if the proposed resources, Non-IT Infrastructure and ICT components are found to be insufficient in meeting the RFP and/or the service level requirements given by OCAC, then we will augment the same without any additional cost to OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:



#### 14.12 Proforma 12: Authorization Letters from all OEMs

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

**Reference:** Supply of equipment/software/License for the project "Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar"

Sir/Madam,

We \_\_\_\_\_, (name and address of the manufacturer) who are established and reputed manufacturers of \_\_\_\_\_ having factories at \_\_\_\_\_ (addresses of manufacturing locations) do hereby authorize M/s \_\_\_\_\_ (name and address of the Bidder) to bid, negotiate and conclude the contract with you against the above mentioned RFP for the above equipment manufactured by us.

Yours faithfully,

For and on behalf of M/s \_\_\_\_\_ (Name of the manufacturer)

Signature \_\_\_\_\_

Name :

Designation :

Address :

Date :

Directorate Seal

---

Note: This letter of authority should be on the letterhead of the concerned manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.

### 14.13 Proforma 13: OEM’s Support Form

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

**Reference:** Supply of equipment/software/license for the project “Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar”

Sir/Madam,

We \_\_\_\_\_, (name and address of the manufacturer) who are established and reputed manufacturers of \_\_\_\_\_ having factories at \_\_\_\_\_ (addresses of manufacturing locations) do hereby assure that we would support our equipment/software/license and freely upgrade them for a period of Five years of Operations and Maintenance, from the date of go-live of the project, by M/s \_\_\_\_\_ (name and address of the Bidder) who has proposed to use for the project “Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar” (OSDC 2.0) or his successor. We would also adhere to the timelines for maintenance as indicated in this RFP by closely working with the Bidder or his successor for a period of five years from the date of supply of the equipment. We abide by the commercials quoted by the Bidder towards AMC charges for five years from the date of supply and successful commissioning of equipment(s) i.e. Go-Live.

We confirm that the products quoted will not be end of life for next seven years from the last date of submission of bids

Yours faithfully,

For and on behalf of M/s \_\_\_\_\_ (Name of the manufacturer)

Signature \_\_\_\_\_

Name :

Designation :

Address :

Date :

Directorate Seal

---

Note: This letter of authority should be on the letterhead of the concerned manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.

#### 14.14 Proforma 14: Warranty Certificate

(On Bidder's Letterhead)

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Sir/Madam,

We warrant that the equipment(s) supplied under the contract would be newly manufactured, free from all encumbrances, defects and faults in material or workmanship or manufacture, shall be of the highest grade and quality, shall be consistent with the established and generally accepted standards for materials of the type ordered, shall be in full conformity with the specifications, drawings of samples, if any, and shall operate as designed. We shall be fully responsible for its efficient and effective operation. We also warrant that the services provided under the contract shall be as per the Service Level Agreement (SLA) with GoO/OCAC.

The obligations under the warranty expressed above shall include all costs relating to labour, spares, maintenance (preventive as well as unscheduled), and transport charges from site to manufacturer's works / service facilities and back for repair or modification or replacement at site of the equipment or any part of the equipment, which under normal care and proper use and maintenance proves defective in design, material or workmanship or fails to operate effectively and efficiently or conform to the specifications and for which notice is promptly given by OCAC to us (Bidder). We shall provide on-site support for all the equipment and services supplied hereunder during the period of this warranty (5 years after acceptance for equipment (5 years for the date of go-live) and entire service period for services).

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

14.15 Proforma 15: Technical specification compliance by OEM/Bidder.

**Minimum Criteria and Condition for OEM/Bidder for Technical Specifications**

The OEM for all the above-mentioned equipment's should be able to support the Warranty and Replacement services efficiently.

Please fill up compliance statement as per below format with Technical Proposal for all items as per Technical specification mentioned in this RFP.

<< OEM Name >> << Table need to modify as per specification table>>

Device Name				
Make				
Model				
S No.	System	Description	Compliance (Y/N)	Remarks

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

#### 14.16 Proforma 16: Statement of No Deviation from Requirement Specifications

RFP Ref. No.: OCAC/\_\_\_\_\_/\_\_\_\_\_

Date:

To  
General Manager (Admin)  
Odisha Computer Application Centre,  
N1/ 7D, Acharya Vihar Square, Near Planetarium,  
P.O. – RRL, Bhubaneswar, Odisha, Pin-751013

Sir,

There are no technical deviations (null deviations) from the requirement specifications of tendered items and schedule of requirements. The entire work shall be performed as per your specifications and documents.

This is to certify that our proposed solution meets all the requirements of the RfP including but not limited to Scope of Work, stated Project Outcomes (including SLAs), Business Requirements and Functional Specifications/ Requirements.

We further certify that our proposed solution meets, is equivalent or better than the minimum technical specifications as given in the RfP.

We understand that the Bill of Quantity provided in the RfP is indicative, we confirm that we have undertaken our own assessment to finalize the components and quantity.

In case, any item of hardware or software is found non-compliant at any stage during project implementation, it would be replaced with a fully compliant product/solution at no additional cost to OCAC. In case of non-adherence of this activity, OCAC reserves the right to cancel the contract, in case the said Contract is awarded to us by OCAC.

We further confirm that our commercial proposal is for the entire scope of work, comprising all required components and our obligations, for meeting the scope of work.

Thanking you,

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

## 14.17 Proforma 17: Bidder's Annual Turnover

**Annual Turnover calculation**

(On the Applicant Statutory Auditors Letterhead)

Date:

This is to certify that we M/s----- are the statutory Auditors of M/s----- and that the below mentioned calculations are true as per the Audited Financial Statements of M/s----- for the below mentioned years.

S No.	Annual Sales Turnover Calculation	2016-17	2017-18	2018-19
1	Total Sales as per the P/L A/c (A)			
2	Less: Custom and/or Excise Duty if included in total Sales as per P/L in Total Sales as per P/L A/C (B)			
3	Less: Sales Tax if included in Total Sales as per P/L A/c (C)			
4	Less: Any other statutory taxes if included in total Sales as per P/L A/C (D)			
5	Less: Any other income from sources other than the normal business source if included in Total Sales as per P/L A/c (E)			
6	Annual Turnover (F) == (A)-(B)-(C)-(D)-(E)			

**The Bidder is required to enclose the audit financial statements for these three years.**

Company Secretary / Statutory Auditor

Name of Signatory:

Bidder Company Name:

Date:

Place:

## 14.18 Proforma 18: Bidder's Net worth

**Net Worth calculation**

(On Applicant's Statutory Auditor's letterhead)

Date:

This is to certify that we M/s----- are the statutory Auditors of M/s----- and that the below mentioned calculations are true as per the Audited Financial Statements of M/s----- for the below mentioned years.

S No.	Annual Sales Turnover Calculation	2016-17	2017-18	2018-19
1	Paid up Share Capital as per B/S (A)			
2	Add: Free Reserves as per B/S (B)			
3	Less: Deferred Payment if any as per B/S (C )			
4	Amount of probable impact on reserves due to audit qualification (D)			
5	Net Worth (F) =(A)+(B)(C)-(D)			
6	Annual Turnover (F) == (A)-(B)-(C)-(D)-(E)			

**Note: Please attach audited Balance Sheets and IT return statements to confirming the figures mentioned in columns.**

Company Secretary / Statutory Auditor

Name of Signatory:

Bidder Company Name:

Date:



## 14.19 Proforma 19: Project Credentials Format

Sl. No.	Item	Detail
<b>General Information</b>		
1.	Customer Name/ Government Department	
2.	Details of Contact Person <ul style="list-style-type: none"> <li>Name:</li> <li>Designation:</li> <li>Email:</li> <li>Phone: &amp; Fax:</li> <li>Mailing Address:</li> </ul>	
<b>Project Details</b>		
3.	Name of the project	
4.	Government/Non-government	
5.	Start Date/End Date	
6.	Current Status	(work in Progress (PAT/FAT/Go-Live) OR completed)
7.	Contract Tenure	
8.	Area of the Data Centre	
9.	Effort involved in Payroll person-months in the complete project	
10.	Order Value of the project (in Crores )	
11.	Please provide copies of Work Order or Certificate of Completion for completed projects from the customer	
More than one same table content may be provided for more than one project detail.		

I do hereby acknowledge that the details provided above are true to best of my knowledge.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

## 14.20 Proforma 21: Format for providing CV of Key Personnel

**Curriculum Vitae of Key Personnel's**

The bidder shall provide the summary table of details of the manpower that will be deployed on this project during the implementation.

**Table-A**

S No	Type of Resource	Name of Resources	Key Responsibilities	Highest Academic Qualifications and Certifications (e.g. PMP/CDCP /ATD/CCNA/ITIL)	Years of Relevant Experience
1	Project Manager				
2	---				
3	---				
4	---				
5	---				
6	Others				
...					

**Table-B**

Sl. No.	Particulars	Details	Supporting document
1.	Key resource / Non Key resource		
2.	Name of the Personal		
3.	Current Designation/Job title		
4.	Current job responsibilities		
5.	Proposed Role in this project		
6.	Total experience and relevant experience (in years)		
7.	Number of years with the organization and date of joining the firm		
8.	Whether resource is engaged by the firm in its own payrolls	YES/NO	
9.	Summary of Professional / Domain Experience		
10.	Date of Birth		
11.	Academic Qualifications: <ul style="list-style-type: none"> <li>• Degree</li> <li>• Academic institution graduated from</li> <li>• Year of graduation</li> <li>• Specialization (if any)</li> </ul>		Attach certificate of highest qualification

Sl. No.	Particulars	Details	Supporting document
	<ul style="list-style-type: none"> <li>Key achievements and other relevant information (if any)</li> </ul>		
12.	Professional Certifications/ Training		Attach relevant certificates
13.	Membership of Professional Associations		
14.	Employment Record*		
15.	<ul style="list-style-type: none"> <li>Details of similar project handled &amp; the role assigned</li> <li>Prior project experience</li> <li>Project name</li> <li>Customer</li> <li>Key project features in brief</li> <li>Location of the project</li> <li>Designation</li> <li>Role</li> <li>Responsibilities and activities</li> <li>Duration of the project</li> </ul>		
16.	Detailed tasks Proposed to be assigned	Work already undertaken that best illustrates capability to handle the tasks assigned**	
17.	Signature of the representative		

I hereby declare that the above mentioned resource would be available during the project phase of this RFP.

\*Starting with present position, list in reverse order every employment held by the staff member since graduation

\*\*Among the assignments in which the staff has been involved, indicate brief details of the project in which this responsibility was assigned (including nature and duration of duty)

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

14.21 Proforma 22: Detailed Timelines and Work Plan with proposed Manpower Strength

The Bidder is supposed to specify a detailed work plan for all activities that will be carried out during the project implementation phase and proposed engagement of manpower strength on monthly basis. Provided below is an indicative work plan.

#	Activities	Months											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Design Validation												
2	Design and OEM Approval by Customer / Consultant												
3	Statutory Approvals (if Any)												
4	Civil & Interior Works												
5	Delivery and Installation of Electricals Low side jobs												
6	Delivery and Installation of Electricals High Side Jobs												
7	Interior Work												
9	Plumbing work												
10	IBMS Low Side Delivery and Installation												
11	HVAC Low Side delivery and Installation												
12	IBMS High side Delivery and Installation												
13	HVAC High Side Delivery and Installation												
14	Delivery and Installation of UPS and Battery												
15	Delivery and Installation of DG												
16	Delivery and Installation of Video Wall												
17	Delivery and Installation of Rack and PDU												
18	Commissioning and Testing of all systems												
19	Handing Over to customer for ICT Installation												
20	SITC of ICT infrastructure												

Indicate all main activities of the assignment, including delivery of reports (e.g. inception, interim and final reports) and other benchmarks such as Customer approvals. Duration of activities shall be indicated in the form of a bar chart. Please specify other activity (Addition or Deletion), if not listed in the form.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

14.22 Proforma 23: Format for Unpriced Bill of Material

S. No.	Product Detail (Parent & it's Child)	Part Code (Parent and Child Item)	Make & Model	UoM	Qty.	Remarks (If Any)
1.						
2.						
3.						
...						

Attach detailed specifications and provide reference number in remarks column.

Thanking you,  
Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

14.23 Proforma 24: Format for Performance for Bank Guarantee (PBG)

Ref. No. \_\_\_\_\_

Bank Guarantee No \_\_\_\_\_

Dated \_\_\_\_\_

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Dear Sir/Madam,

In consideration of Odisha Computer Application Centre, OCAC tower, Bhubaneswar – 751013, Odisha, India, India (hereinafter referred to as 'OCAC', which expression shall, unless repugnant to the context or meaning thereof, include all its successors, administrators, executors and assignees) after receipt of the Letter of Intent (LOI) dated \_\_\_\_\_ with M/s \_\_\_\_\_ having it's registered / head office at \_\_\_\_\_ (hereinafter referred to as the SYSTEMS INTEGRATOR) which expression shall, unless repugnant to the context or meaning thereof include all its successors, administrators, executors and assignees) and OCAC having agreed that the SYSTEM INTEGRATOR shall furnish to OCAC a performance guarantee for 10% of the Total Project Cost for the faithful performance of the entire contract.

We (name of the bank) \_\_\_\_\_ registered under the laws of \_\_\_\_\_ having head / registered office at \_\_\_\_\_ (hereinafter referred to as "the Bank", which expression shall, unless repugnant to the context or meaning thereof, include all its successors, administrators, executors and permitted assignees) do hereby guarantee and undertake to pay immediately on first demand in writing any / all moneys to the extent of 10% of the Total Project Cost without any demur, reservation, contest or protest and / or without any reference to the SYSTEMS INTEGRATOR. Any such demand made by OCAC on the Bank by serving a written notice shall be conclusive and binding, without any proof, on the bank as regards the amount due and payable, notwithstanding any dispute(s) pending before any Court, Tribunal, Arbitrator or any other authority and / or any other matter or thing whatsoever, as liability under these presents being absolute and unequivocal. We agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged by OCAC in writing. This guarantee shall not be determined, discharged or affected by the liquidation, winding up, dissolution or insolvency of the SYSTEM INTEGRATOR and shall remain valid, binding and operative against the bank.

The Bank also agrees that OCAC at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance, without proceeding against the SYSTEM INTEGRATOR and notwithstanding any security or other guarantee that OCAC may have in relation to the SYSTEMS INTEGRATOR's liabilities.

The Bank further agrees that OCAC shall have the fullest liberty without our consented without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the said SYSTEMS INTEGRATOR(s) from time to time or to postpone for any time or from time to time exercise of any of the powers vested in OCAC against the said SYSTEMS INTEGRATOR(s) and to forbear or enforce any of the terms and conditions relating to

the said agreement and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said SYSTEMS INTEGRATOR(s) or for any forbearance, act or omission on the part of OCAC or any indulgence by OCAC to the said SYSTEMS INTEGRATOR(s) or any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

The Bank further agrees that the Guarantee herein contained shall remain in full force during the period that is taken for the performance of the contract and all dues of OCAC under or by virtue of this contract have been fully paid and its claim satisfied or discharged or till OCAC discharges this guarantee in writing, whichever is earlier.

This Guarantee shall not be discharged by any change in our constitution, in the constitution of OCAC or that of the SYSTEMS INTEGRATOR.

The Bank confirms that this guarantee has been issued with observance of appropriate laws of the country of issue.

The Bank also agrees that this guarantee shall be governed and construed in accordance with Indian Laws and subject to the exclusive jurisdiction of Indian Courts of OCAC.

Notwithstanding anything contained herein above, our liability under this Guarantee is limited to Indian Rs. (in figures) \_\_\_\_\_ (Indian Rupees (in words) \_\_\_\_\_) and our guarantee shall remain in force until \_\_\_\_\_ (indicate OCAC date of expiry of bank guarantee). Any claim under this Guarantee must be received by us before the expiry of this Bank Guarantee. If no such claim has been received by us by the said date, the rights of OCAC under this Guarantee will cease. However, if such a claim has been received by us within the said date, all the rights of OCAC under this Guarantee shall be valid and shall not cease until we have satisfied that claim.

In witness whereof, the Bank through its authorized officer has set its hand and stamp on this \_\_\_\_\_ Day of \_\_\_\_\_ 2020 at \_\_\_\_\_



## 14.24 Proforma 25: Format of Commercial Proposal Document

Format for reporting commercials and mandatory letters that needs to be part of the commercial proposal document. Breakdown of cost mentioned, cost of each component, operating cost, employee cost, cost of operations and management, any other cost which the Bidder feels.

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

**Subject:** Submission of Commercial proposal for "Selection of System Integrator for Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar".

**Reference:** RFP No: **OCAC/\_\_\_\_\_/\_\_\_\_** Dated: **\_\_\_/\_\_\_/\_\_\_\_\_**

We, the undersigned Bidder, having read and examined in detail the RFP documents for "RFP for Selection of System Integrator for "Design, Build, Installation, Commissioning, Integration and Operation & Maintenance of Non-IT & IT infrastructure for Extension of Odisha State Data Centre at OCAC Tower, Bhubaneswar, (OSDC 2.0)". I / we do hereby propose to provide services as specified in the RFP documents number **OCAC/\_\_\_\_\_/\_\_** **Dated** **\_\_\_/\_\_\_/\_\_\_\_\_**

### 1. PRICE PROPOSAL AND VALIDITY

All the prices mentioned in our RFP are in accordance with the terms as specified in the RFP documents. All the prices and other terms and conditions of this RFP are valid for a period of 180 days as desired in the RFP

We hereby confirm that our RFP prices include all taxes. However, all the taxes are quoted separately under relevant sections.

We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other corporate Tax in altered under the law, we shall pay the same.

### 2. UNIT RATES

We have indicated in the relevant schedules enclosed the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

### 3. DEVIATIONS

We declare that all the services shall be performed strictly in accordance with the RFP documents except for the variations and deviations, all of which have been detailed out exhaustively in the following statement, irrespective of whatever has been stated to the contrary anywhere else in our

proposal. Further, we agree that additional conditions, if any, found in the RFP documents, other than those stated in deviation schedule, shall not be given effect to.

**4. RFP PRICING**

We further confirm that the prices stated in our proposal are in accordance with your Instruction to Bidders included in RFP documents.

**5. QUALIFYING DATA**

We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our RFP, we agree to furnish the same in time to your satisfaction.

**6. PROPOSAL PRICE**

We declare that our Proposal Price is for the entire scope of the work as specified in the Schedule of Requirements and RFP documents.

**7. PERFORMANCE BANK GUARANTEE BOND**

We hereby declare that in case the contract is awarded to us, we shall submit the PBG bond in the form prescribed in Proforma of Bank Guarantee towards PBG and as per General Conditions of Contract. We hereby declare that our RFP is made in good faith, without collusion or fraud and the information contained in the RFP is true and correct to the best of our knowledge and belief. We understand that our RFP is binding on us and that you are not bound to accept a RFP you receive. We confirm that no Technical deviations are attached here with this commercial offer.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name: \_\_\_\_\_ Place: \_\_\_\_\_

Designation: \_\_\_\_\_ Date: \_\_\_\_\_

## 14.25 Proforma 26: Undertaking on Exit Management and Transition

### Undertaking on Exit Management and Transition

(On the Bidder's Letterhead)

RFP Ref. No: OCAC/\_\_\_\_\_/\_\_\_\_

Date:

**To**  
**General Manager (Admin)**  
**Odisha Computer Application Centre,**  
**N1/ 7D, Acharya Vihar Square, Near Planetarium,**  
**P.O. – RRL, Bhubaneswar, Odisha, Pin-751013**

Dear Sir/Madam,

**Sub:** Undertaking on Exit Management and Transition

1. I/We hereby undertake that at the time of completion of our engagement with OCAC, either at the End of Contract or termination of Contract before planned Contract Period for any reason, we shall successfully carry out the exit management and transition of this Project to OCAC or to an agency identified by OCAC to the satisfaction of OCAC. I/We further undertake to complete the following as part of the Exit management and transition:
  - a. We undertake to complete the updating of all Project documents and other artefacts and handover the same to OCAC before transition.
  - b. We undertake to design standard operating procedures to manage system (including application and IT systems), document the same and train OCAC personnel on the same.
  - c. If OCAC decides to take over the operations and maintenance of the Project on its own or identifies or selects any other agency for providing operations & maintenance services on this Project, then we shall provide necessary handholding and transition support, which shall include but not be limited to, conducting detailed walkthrough and demonstrations for the IT Infrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the ICT components , conducting Training sessions etc.
2. I/We also understand that the Exit management and transition will be considered complete on the basis of approval from OCAC.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date

## Annexure -A (As-Is Inventory List of Current SDC )

## Server Detail

SL	Server Name	Server Type	Make	Model	Installed OS
1	HYPER-V SERVER	OSDCMHV 08	IBM	BL-HS22	Microsoft Hyper-V Server 2012
2	ADDITIONAL DOMAIN CONTROLLER SERVER	ADC	IBM	BL-HS22	Windows 2008 Enterprise
3	HYPER-V SERVER	OSDCMHV 12	IBM	BL-HS22	Microsoft Hyper-V Server 2012
4	PROXY SERVER	PROXY-2	IBM	BL-HS22	Windows 2008 Enterprise
5	HYPER-V SERVER	OSDCMHV 10	IBM	BL-HS22	Microsoft Hyper-V Server 2012
6	DATABASE SERVER ON AIX PLATFORM	OSDCDBA 01	IBM	P-550	AIX 7.1
7	DATABASE SERVER ON AIX PLATFORM	OSDCDBA 02	IBM	P-550	AIX 7.1
8	DATABASE SERVER ON AIX PLATFORM	OSDCDBA 03	IBM	P-550	AIX 7.1
9	DATABASE SERVER ON WINDOWS PLATFORM	OSDCDBW 01	IBM	X-3850 M2	Windows 2008 Enterprise
10	DATABASE SERVER ON WINDOWS PLATFORM	OSDCDBW 02	IBM	X-3850 M2	Windows 2008 Enterprise
11	TIVOLI STORAGE MANAGEMENT SERVER	OSDCTSM	IBM	X-3850 M2	Windows 2008 Enterprise
12	STAGGING SERVER	OSDCSTG W01	IBM	X-3850 M2	Windows 2008 Enterprise
13	CA TIM SERVER	OSDCTIM	IBM	X-3850 M2	RHEL 5.5 FOR CA TIM
14	ORACLE RAC SERVER	OSDCDBA 04	IBM	P-550	AIX 6.1
15	HYPER-V SERVER	OSDCMHV 05	IBM	BL-HS22	Microsoft Hyper-V Server 2012

SL	Server Name	Server Type	Make	Model	Installed OS
16	APPLICATION SERVER ON WINDOWS PLATFORM	OSDCWAP W12	IBM	BL-HS22	Windows 2008 Enterprise
17	HYPER-V SERVER	OSDCMHV 06	IBM	BL-HS22	Microsoft Hyper-V Server 2012
18	HYPER-V SERVER	OSDCMHV 11	IBM	BL-HS22	Microsoft Hyper-V Server 2012
19	NETWORK FAULT MANAGEMENT SERVER	EMSNFM	IBM	BL-HS22	windows 2003 Enterprise
20	NETWORK PERFORMANCE MANAGEMENT SERVER	EMSNPM	IBM	BL-HS22	windows 2003 Enterprise
21	HELPDESK SERVER	EMSHD	IBM	BL-HS22	windows 2003 Enterprise
22	SERVER MANAGEMENT SERVER	EMSSM	IBM	BL-HS22	windows 2003 Enterprise
23	DATABASE MANAGEMENT SERVER	EMSDM	IBM	BL-HS22	windows 2003 Enterprise
24	ORACLE RAC SERVER	OSDCDBA 05	IBM	P-550	AIX 6.1
25	HYPER-V SERVER	OSDCMHV 09	IBM	BL-HS22	Microsoft Hyper-V Server 2012
26	WEB APPLICATION SERVER ON WINDOWS PLATFORM	OSDCWAP W2	IBM	BL-HS22	Windows 2008 Enterprise
27	HYPER-V SERVER	OSDCMHV 07	IBM	BL-HS22	Microsoft Hyper-V Server 2012
28	WEB APPLICATION SERVER ON WINDOWS PLATFORM	OSDCWAP W14	IBM	BL-HS22	Windows 2008 Enterprise
29	IBM BLADE CHASIS	NA	IBM	MT 8677	NA
30	IBM BLADE CHASIS	NA	IBM	MT 8677	NA
31	HYPER-V SERVER	OSDCMHV 04	IBM	BL-HS23	Microsoft Hyper-V Server 2012
32	HYPER-V SERVER	OSDCMHV 03	IBM	BL-HS23	Microsoft Hyper-V Server 2012
33	HYPER-V SERVER	OSDCMHV 01	IBM	BL-HS23	Microsoft Hyper-V Server 2012

SL	Server Name	Server Type	Make	Model	Installed OS
34	HYPER-V SERVER	OSDCMHV 02	IBM	BL-HS23	Microsoft Hyper-V Server 2012
35	HYPER-V SERVER	OSDCDBW 03	HP	BL460C G9	Windows 2016 Server Std.
36	HYPER-V SERVER	OSDCDBW 04	HP	BL460C G9	Windows 2016 Server Std.
37	HYPER-V SERVER	OSDCMHV 23	HP	BL460C G9	Microsoft Hyper-V Server 2012 R2
38	HYPER-V SERVER	OSDCMHV 24	HP	BL460C G9	Microsoft Hyper-V Server 2012 R2
39	HYPER-V SERVER	OSDCMHV 25	HP	BL460C G9	Microsoft Hyper-V Server 2012 R2
40	HYPER-V SERVER	OSDCMHV 26	HP	BL460C G9	Microsoft Hyper-V Server 2012 R2
41	HYPER-V SERVER	OSDCMHV 27	HP	BL460C G9	Microsoft Hyper-V Server 2012 R2
42	HYPER-V SERVER	OSDCMHV 28	HP	BL460C G9	Microsoft Hyper-V Server 2012 R2
43	HP BLADE CHASIS	NA	HP	BLC 7000C	NA
44	ESXi Server	OSDCMGM THV01	HP	HPEDL 380	ESXi 6.7 Bare Metal
45	ESXi Server	OSDCMGM THV02	HP	HPEDL 380	ESXi 6.7 Bare Metal
46	ESXi Server	OSDCMGM THV03	HP	HPEDL 380	ESXi 6.7 Bare Metal
47	ESXi Server	OSDCMGM THV04	HP	HPEDL 380	ESXi 6.7 Bare Metal
48	ESXi Server	OSDCPRO DHV01	HP	HPEDL 380	ESXi 6.7 Bare Metal
49	ESXi Server	OSDCPRO DHV02	HP	HPEDL 380	ESXi 6.7 Bare Metal
50	ESXi Server	OSDCPRO DHV03	HP	HPEDL 380	ESXi 6.7 Bare Metal
51	ESXi Server	OSDCPRO DHV04	HP	HPEDL 380	ESXi 6.7 Bare Metal

SL	Server Name	Server Type	Make	Model	Installed OS
52	ESXi Server	OSDCPRO DHV05	HP	HPEDL 380	ESXi 6.7 Bare Metal
53	ESXi Server	OSDCPRO DHV06	HP	HPEDL 380	ESXi 6.7 Bare Metal
54	ESXi Server	OSDCSTG HV01	HP	HPEDL 380	ESXi 6.7 Bare Metal
55	ESXi Server	OSDCSTG HV02	HP	HPEDL 380	ESXi 6.7 Bare Metal

## Network Equipment

S No	Item Description	Make	Model	Type
1	INTERNET ROUTER	CISCO	CISCO3845	NA
2	INTERNET ROUTER	CISCO	CISCO3845	NA
3	INTERNET SWITCH	CISCO	Cat3560G-24TS	NA
4	INTERNET SWITCH	CISCO	Cat3560G-24TS	NA
5	NETWORK LOADBALANCER	RADWARE	LinkProof On Demand Switch 2	NA
6	NETWORK LOADBALANCER	RADWARE	LinkProof On Demand Switch 2	NA
7	IPS	RADWARE	DP-1016-NL-D-Q	NA
8	IPS	RADWARE	DP-1016-NL-D-Q	NA
9	INTERNET FIREWALL	CISCO	Cisco ASA5580	NA
10	INTERNET FIREWALL	CISCO	Cisco ASA5580	NA
11	CORE SWITCH	CISCO	WS-C6509-E	NA
12	CORE SWITCH	CISCO	WS-C6509-E	NA
13	WEB DMZ SWITCH	CISCO	Cat3560G-24TS	NA
14	WEB DMZ SWITCH	CISCO	Cat3560G-24TS	NA
15	APP LOADBALANCER	RADWARE	AppDirector with Cookie Persistency	NA
16	APP LOADBALANCER	RADWARE	AppDirector with Cookie Persistency	NA
17	INTRANET FIREWALL	CISCO	Cisco ASA5550	NA
18	INTRANET FIREWALL	CISCO	Cisco ASA5550	NA
19	MGM DMZ SWITCH	CISCO	Cat3560G-24TS	NA
20	MGM DMZ SWITCH	CISCO	Cat3560G-24TS	NA
21	APP & DB DMZ SWITCH	CISCO	Cat3560G-24TS	NA
22	APP & DB DMZ SWITCH	CISCO	Cat3560G-24TS	NA
23	ACCESS SWITCH	CISCO	Cat3560G-24TS	NA
24	Access Control Server (AAA Server)	CISCO	Cisco 1120 Secure ACS	NA
25	Access Control Server (AAA Server)	CISCO	Cisco 1120 Secure ACS	NA
26	MAIL SECURITY APPLIANCE	SYMANTEC	SYMANTEC MAIL SECURITY 8340 APPLIANCE	NA
27	MAIL SECURITY APPLIANCE	SYMANTEC	SYMANTEC MAIL SECURITY 8340 APPLIANCE	NA
28	KVM Switch	IBM	IBM 17353LX	NA
29	KVM Switch	IBM	IBM 17353LX	NA
30	KVM Switch	IBM	IBM 17353LX	NA
31	ArcSight ESM Express	HP	HP DL380 Gen9	NA
32	ArcSight Logger1	HP	HP DL360 Gen9	NA
33	ArcSight Logger2	HP	HP DL360 Gen9	NA
34	ArcSight Connector Server1	HP	HP DL360 Gen9	NA
35	ArcSight Connector Server2	HP	HP DL360 Gen9	NA
36	ArcSight UBA	HP	HP DL380 Gen9	NA
37	INTRANET FIREWALL	CISCO	CISCO FBR9K-SM-S800GS1	NA
38	FMC	CISCO	CISCO FIREPOWER MANAGEMENT CENTRE 2500	NA
39	NXS SWITCH	CISCO	CISCO NEXUS N9K-C93180YC-FX	NA



S No	Item Description	Make	Model	Type
40	NXS SWITCH	CISCO	CISCO NEXUS N9K-C93180YC-FX	NA
41	NXS SWITCH	CISCO	CISCO NEXUS N9K-C93180YC-FX	NA
42	NXS SWITCH	CISCO	CISCO NEXUS N9K-C93180YC-FX	NA
43	INTRANET FIREWALL	CISCO	CISCO FBR9K-SM-S800GS1	NA
44	IPS	RADWARE	RADWARE DEFENSEPRO	NA
45	IPS	RADWARE	RADWARE DEFENSEPRO	NA
46	APP LOADBALANCER	RADWARE	RADWARE ALTEON 6024	NA
47	APP LOADBALANCER	RADWARE	RADWARE ALTEON 6024	NA
48	VPN	CISCO	CISCO ASA 5525	NA
49	VPN	CISCO	CISCO ASA 5525	NA

## Storage Equipment Details.

S No	Name	Type	Make	Model
1	SAN Switch	NA	CISCO	DS-C9134-K9
2	SAN Switch	NA	CISCO	DS-C9134-K9
3	SAN Switch	NA	CISCO	DS-C9134-K9
4	SAN Switch	NA	CISCO	DS-C9134-K9
5	Storage	1818-53A	IBM	DS 5300
6	Storage Disk Self	1818-D1A	IBM	EXP 5000
7	Storage Disk Self	1818-D1A	IBM	EXP 5000
8	Storage Disk Self	1818-D1A	IBM	EXP 5000
9	Storage Disk Self	1818-D1A	IBM	EXP 5000
10	Storage Disk Self	1818-D1A	IBM	EXP 5000
11	Storage Disk Self	1818-D1A	IBM	EXP 5000
12	Storage Disk Self	1818-D1A	IBM	EXP 5000
13	Storage Disk Self	1818-D1A	IBM	EXP 5000
14	Storage Disk Self	1818-D1A	IBM	EXP 5000
15	Storage Disk Self	1818-D1A	IBM	EXP 5000
16	Storage Disk Self	1818-D1A	IBM	EXP 5000
17	Storage Disk Self	1818-D1A	IBM	EXP 5000
18	Storage Disk Self	1818-D1A	IBM	EXP 5000
19	Storage Disk Self	1818-D1A	IBM	EXP 5000
20	VTL Disk self	3955SV6	IBM	TS 7520
21	VTL Disk self	3955SX6	IBM	TS 7520
22	VTL Disk self	3955SX6	IBM	TS 7520
23	VTL Disk self	3955SX6	IBM	TS 7520
24	VTL Disk self	3955SV6	IBM	TS 7520
25	VTL Disk self	3955SX6	IBM	TS 7520
26	VTL Disk self	3955SX6	IBM	TS 7520
27	VTL Disk self	3955SX6	IBM	TS 7520
28	VTL Disk self	3955SV6	IBM	TS 7520
29	VTL Disk self	3955SX6	IBM	TS 7520
30	VTL Disk self	3955SV6	IBM	TS 7520
31	VTL Disk self	3955SX6	IBM	TS 7520

S No	Name	Type	Make	Model
32	VTL Base server -1	3954-CV7	IBM	TS 7500 SERVER
33	VTL Base server -2	3954-CV7	IBM	TS 7500 SERVER
34	Tape Library	3576-L5B	IBM	IBM LT04 UDS3
35	Tape Library expansion	3576-69U	IBM	IBM LT04 UDS3
36	Hitachi VSP Replicator	NA	HITACHI	HJ-4230-7EWEA
37	Brocade Switch	NA	Brocade	Brocade 7800
38	Brocade Switch	NA	Brocade	Brocade 7800
39	MDS/SAN Switch	NA	Cisco	DSC9148-32P-K9
40	MDS/SAN Switch	NA	Cisco	DSC9148-32P-K9
41	SAN STORAGE	NA	DELL	SC 7020
42	NAS	NA	DELL	FS 8600
43	SAN Switch	NA	HPE	HPSN6500B
44	SAN Switch	NA	HPE	HPSN6500B
45	SAN STORAGE	NA	HPE	HPE 3 PAR 8440
46	Storage Disk Self	NA	HPE	HPE 3 PAR 8000
47	Storage Disk Self	NA	HPE	HPE 3 PAR 8000
48	Storage Disk Self	NA	HPE	HPE 3 PAR 8000
49	Storage Disk Self	NA	HPE	HPE 3 PAR 8000
50	Storage Disk Self	NA	HPE	HPE 3 PAR 8000
51	Storage Disk Self	NA	HPE	HPE 3 PAR 8000
52	Storage Disk Self	NA	HPE	HPE 3 PAR 8000
53	Storage Disk Self	NA	HPE	HPE 3 PAR 8000
54	StoreServ SPS Service Processor	NA	HPE	HPE ProLiantDL120 Gen9

### Current Desktop, Laptop & Printer details

S No	Type	Make	Model
1	Desktop	DELL	OPTIPLEX 380
2	Desktop	DELL	OPTIPLEX 380
3	Desktop	DELL	OPTIPLEX 380
4	Desktop	DELL	OPTIPLEX 380
5	Desktop	DELL	OPTIPLEX 380
6	Desktop	DELL	OPTIPLEX 380
7	Desktop	DELL	OPTIPLEX 380
8	Desktop	DELL	OPTIPLEX 380
9	Desktop	DELL	OPTIPLEX 380
10	Desktop	DELL	OPTIPLEX 380
11	Desktop	HP	HP COMPAQ DX2480
12	Desktop	DELL	OPTIPLEX 9010
13	Desktop	DELL	OPTIPLEX 9010
14	Desktop	DELL	OPTIPLEX 9010
15	Desktop	DELL	OPTIPLEX 9010
16	Desktop	DELL	OPTIPLEX 9010
17	Desktop	DELL	OPTIPLEX 9010

18	Laptop	Dell	VOSTRO 1015
19	Laptop	Dell	VOSTRO 1015
20	Laptop	Dell	VOSTRO 1015
21	Laptop	Dell	VOSTRO 1015
22	Laptop	Dell	VOSTRO 1015
23	Laptop	Dell	VOSTRO 3460
24	Laptop	Dell	VOSTRO 3460
25	Laptop	Dell	VOSTRO 3460
26	Laptop	Dell	VOSTRO 3460
27	LASER PRINTER	HP	HPDV-MFD
28	LASER PRINTER	HP	HPDV-MFD
29	BMS Printer (Inkjet)	HP	HP DESKJET D 2668