ANNEXURE - B

Updated Technical Specification for Odia University

1. Specifications of 86" Interactive Digital Board		
Sl.No	**Features**	**Specifications Required**
1	Screen Size	86" or Higher
2	Native Resolution	3840 x 2160 (UHD)
3	Brightness	Minimum 350cd/m2 or higher
4	Contrast Ratio	1,100:1 or Higher
5	Viewing Angle(H x V)	178 x 178
6	Surface Treatment	Anti-glare treatment or similar
7	Min Input ports	HDMI x 2(with HDCP 2.2), USB 3.0 x 4, USB 2.0 x1, USB(Type C x1 with power delivery and DP Alt Mode), OPS Slot x 1
8	Min Output Ports	Audio-1(Audio out to connect additional Speakers if required), Optical SPDIF x1, HDMI-1, Touch Out USB x 2
9	External Control	RS232C, RJ45 input and output both
10	Built in Touch type	IR/IR spread /P Cap/Incell/In glass
11	Touch Accuracy	±1mm or less
12	Air Gap Between LCD Module & Glass	Minimum 1 mm or less
13	Protection Glass Thickness	3T (Anti-Glare) or Higher
14	Operating System Support	Windows 7/8/10/Windows XP/ Linux/ Mac/ Android(Windows XP/ Linux/ Mac Support one point touch)
15	Multi touch point	Min 20 Points or Higher
18	Interactive Features	White Board & Standard Interactive features
		Writing, Pen,Palm Eraser ,Screen Capture, Storage, Tool Bar,Air Class for Online test/Quiz,USB Block feature for safety, Dual Pen support,Bluetooth connectivity.
18	Built in Standard OS	Android 11/Tizen 6.5/ Web OS
19	Key Hardware Features	Minimum Internal Memory (32GB), Quad core A55 , GPU-Mali G52MP2, RAM DDR 4GB or higher, USB Block, Anti Glare Coating on glass surface, 7 Mohs and 9H Hardness, Haze 28%
20	Key Software Features	Screen Share/Mira cast to Connect TAB/Mobile, Web Browser ,Wi-Fi, Apple Airplay inbuilt, Booting Logo Image Change Option, Able to connect and show upto 9 devices wirelessly on screen, DMS software option from same OEM of display, PIP, PBP, Wake on LAN, Able to open and work on

		minimum 4 applications side by side on one screen at a time.
22	PCB Protective Coating	Conformal Coating on PCB to prevent from Humidity, Dust & Iron Particles
23	Power Supply	100-240V~, 50/60Hz
24	Power Consumption (Typ.)	385W or less
24	Built in Audio Power	30W (15W x 2)/10W X 4
25	Product Quality Certifications	BIS, ISO9001,ISO14001,ISO45001
26	Accessory	Remote Controller(include battery 2ea), Power Cord, QSG, Regulation Book, Touch Pen(2)
27	Warranty	3 years
28	Bracket	Wall mount

2. Firewall

Hardware Architecture & Performance
The appliance based security platform should be capable of providing firewall, application visibility, Web Protection and IPS functionality in a single appliance
The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support minimum 8GB memory. Should have dedicated network processor with additional RAM for hardware acceleration.
Should support minimum 120 GB SSD for logs & reports
The appliance should support atleast 8 * 1G ports 2 * 1G SFP ports from day 1 . The appliance should have option to support additional 4 * 10G ports in future.
Should support atleast 24 Gbps Firewall throughput & 5 Gbps of NGFW throughput
Proposed appliance should support at least 3 million concurrent sessions or more
Firewall should support atleast 125K connections per second or more
Solution should have 11 Gbps of IPSec VPN throughput
Firewall Should support atleast 1Gbps of Threat Protection Throught (Measured with Firewall, IPS, Application Control, and Malware prevention enabled)
Solution should have 1.4Gbps SSL/TLS inspection throughput & 2500 SSL VPN concurrent tunnel
Industry Certification
Solution should have FIPS & TEC certified
Solution should provide make in India certificate with minimum 60% local content
Solution should have common criteria EAL4+ certified
General Management
Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators
Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN
Firewall should support TLS 1.3 inspection of encrypted traffic

Firewall should support technology for application acceleration
Firewall should be ready for Detection & Response and SDWAN from day one.
High Availability (HA) support clustering two devices in active-active or active-passive mode.
Full command-line-interface (CLI) accessible from GUI
Automated firmware update notification with easy automated update process and roll-back features
Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers
Jumbo Frame Support , Self-service user portal
SNMPv3 and Netflow support , API for 3rd party integration
Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
Firewall, Networking & Routing
Stateful deep packet inspection firewall
Network Flow FastPath acceleration for trusted traffic
User, group, time, or network based policies
Access time polices per user/group
Enforce policy across zones, networks, or by service type
Zone isolation and zone-based policy support
Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi
Custom zones on LAN or DMZ
Customization NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule
Flood protection: DoS, DDoS and portscan blocking Country blocking by geo-IP
Routing: static, multicast (PIM-SM), and dynamic (RIP, BGP, OSPF)
Protocol independent multicast routing with IGMP snooping
Bridging with STP support and ARP broadcast forwarding
VLAN DHCP support and tagging,VLAN bridge support
WAN link balancing: multiple Internet connections, auto-link health check, automatic fail over, automatic and weighted balancing, and granular multipath rules
Full configuration of DNS, DHCP and NTP, 802.3ad interface link aggregation
IPv6 tunneling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment through IPSec
Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription)
Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
Authentication
Synchronized User ID utilizes Synchronized Security to share currently logged in Active Directory user ID between endpoints and the firewall without an agent on the AD server or client

Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
Server authentication agents for Active Directory SSO, STAS, SATC
Single sign-on: Active directory, eDirectory, RADIUS Accounting
Client authentication agents for Windows, Mac OS X, Linux 32/64
Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos
Browser Captive Portal
Authentication certificates for iOS and Android
Authentication services for IPSec, SSL, L2TP, PPTP
Google Chromebook authentication support for environments with Active Directory and Google G Suite
Next Gen VPN Support
Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
L2TP and PPTP, Route-based VPN
Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Android VPN client support, IKEv2 Support
SSL client for Windows and configuration download through user portal/ GUI Interface/OEM portal.
Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC
Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
The solution should support enabling synchronized the client security posture for remote users when same OEMs End point protection is installed"
Unlimited IPSec & SSL client with unlimited 2factor mobile (android & IOS) authenticator license
Single client support for IPSec & SSL remote VPN
Mac and Windows Support
Wireless Protection
Wireless controller with 50 access point management license from day1
Multiple SSID support per radio including hidden SSIDs
Bridge APs to LAN, VLAN, or a separate zone with client isolation options
Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support
Support for 802.11r (fast transition)
Hotspot support for (custom) vouchers, password of the day, or T&C acceptance
Wireless guest Internet access with walled garden options
Time-based wireless network access
The solution should support bridging and mesh mode with supported AP.
Intrusion Prevention (IPS)
High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection
Minimum 5000 of signatures, Support for custom IPS signatures

Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
Endpoints should identify including the host, user, process, incident count, and time of compromise
Security policies can limit access to network resources or completely isolate compromised systems until they are cleaned
Lateral Movement Protection further isolates compromised systems by having healthy - managed endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain
Web Protection and Control
Fully transparent proxy for anti-malware and web-filtering
Enhanced Advanced Threat Protection
URL Filter database with millions of sites across 92 categories backed by OEM Labs
Surfing quota time policies per user/group ,Access time polices per user/group
Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email
Advanced web malware protection with JavaScript emulation
Live Protection real-time in-the-cloud lookups for the latest threat intelligence
Second independent malware detection engine for dual-scanning
HTTP and HTTPS scanning on a per user or network policy basis with customization rules and exceptions
File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)
YouTube for Schools enforcement per policy (user/group)
SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)
Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists
Block Potentially Unwanted Applications (PUAs)
Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users
User/Group policy enforcement on Google Chromebooks
Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
Application Protection and Control
Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints and the firewall
Signature-based application control with patterns for thousands of applications
Cloud Application Visibility and Control to discover Shadow IT
Smart Filters that enable dynamic policies which automatically update as new patterns

Micro app discovery and control
Application control based on category, characteristics (e.g., bandwidth and productivity consuming),technology (e.g. P2P), and risk level
Per-user or network rule application control policy enforcement
Zero Day Protection
Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
Aggressive behavioral, network, and memory analysis
Suspicious files subjected to threat intelligence analysis in parallel with full sandbox analysis
Machine Learning technology with Deep Learning scans all dropped executable files
Includes exploit prevention and Cryptoguard Protection technology from endpoint security
In-depth malicious file reports and dashboard file release capability
Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis
Sandboxing enginee should have powered by AI analysis engine
License Includes :
Network Protection Subscriptions (IPS,HTML5, ATP, Anti-malware),
Web Protection Subscriptions (URL, AppCtrl, Web/App Traffic Shaping),
Zero Day Protection
24 X 7 hardware & warranty support from OEM