FEDERAL OMBUDSPERSON SECRETARIAT FOR PROTECTION AGAINST HARASSMENT

وفاقی محتسب

OMBUDSPERSON

برائے انسداد ہراسیت

Tender document for	**PURCHASE OF IT EQUIPMENTS/PLANT & MACHINERY/HARDWARE**
Tender document No.	________/FOSPAH/Gen/Proc/ IT Equipments/Plant & Machinery/Hardware /2025-26/.

Office of the Federal Ombudsperson Secretariat for Protection against Harassment of Women at Workplace
LG & RD Complex, First Floor, Sector G-5/2, Islamabad
Telephone No.051-9262953

GENERAL INSTRUCTIONS & CONDITIONS FOR THE BIDDERS

1.	Only those firms are allowed to participate in the tender who are General Sales Tax (GST) registered and have National Tax Number (NTN).
2.	Bidder(s) must have sound financial position, sufficient experience, well reputation and capability for timely completion of supply.
3.	Earnest Money **in the form of Cheque** shall not be accepted, it should be in the form of Pay Order.
4.	No bidder will be allowed to submit its second or third offer with the same bid.
5.	Only those Bid(s) will be considered which would be submitted on the E-PAD.
6.	**Bid opening Procedure.** Single stage- Two envelope method will be adopted to evaluate the offer(s). 40% weightage will be given to ‘Quality’ (i. Related Work experience with govt. organizations(List of Supply orders & work completion certificates) ii. Human Resource (Sales rep. & Technical team etc), iii. Annual Turnover, iv. Quality/Specs of the quoted items) , & 60% weightage will be given to ‘Cost’/ ‘Price’.
7.	Offer(s)/item(s) which were not found according to the standard/specification(s) and evaluation criteria shall not be accepted.
8.	Sample of each item will be approved after detail inspection by the purchase committee.
9.	The offered price of item(s) should be inclusive of General Sales Tax if applicable. Moreover, GST & Income Tax will be deducted according to government rules & regulations.
10.	Validity of Bid shall be up to 30th June 2026.
11.	Bidder(s) must attach General Sales Tax (GST) registration certificate and National Tax Number (NTN).
12.	Bank Account ________________________ & IBAN No ________________________ Vender No.________________________ Name of Bank ____ Address____ Telephone No.____________________ Email address ____________________________________
13.	Pay Order/Call Deposit Receipt of Rs.____________bearing No.___________ dated_________________ of Bank_________________________________ is attached in original as 150,000/-(One Hundred & fifty thousand only) fixed earnest money in favor of DDO, FOSPAH Islamabad as earnest money & performance guarantee will be 2 % for successful bidders.
14.	Payment will be claimed after supply as per tender specifications .
15.	Successful bidder(s) shall deposit 1% of the total value of contract money as performance guarantee in shape of Pay Order or Call Deposit Receipt which will be retained by the department till expiry of guarantee period.
16.	In case any of the terms and conditions of the agreement is violated, the responsibility for any loss or damage shall lie on the supplier firm.

17.	FOSPAH's shall have the right at any stage to change (increase/decrease) the required quantity of the items or cancel the agreement /items without assigning the reason thereof.
18.	If there is any issue on Quality of any item, then final decision will be of the Procurement Committee (FOSPAH).
19.	There will be item wise selection.
20.	Focal Person from applied firm must visit FOSPAH office, LG & RD Complex, First Floor, Sector G-5/2, Islamabad to assess the actual requirements regarding installation/configuration before quoting rates.
21.	Items will be selected on the basis of approved sample/quality.
22.	Any item of tender can be cancelled without giving any reason.
23.	The closing date for submission of E-bids is 05-12-2025 at 2:30 PM and E bid opening time will be 3.00 PM.

Special Instructions for submitting the bid against the items mentioned at Serial No. 28 - 32

SCOPE OF WORK

i) Hardware /software etc installation, configuration and support services will be solely responsibility of the vendor.

ii) Software bidder will be responsible for the installation, configuration and support services.

iii) **In case of any discrepancy** or less item bid will be rejected. Compliance/ Checklist sheet with the Technical specification must be attached with the Technical proposal.

iv) In case of failure or malfunctioning of hardware equipment/component, a free replacement and installation of the device/part will be the responsibility of the vendor and on exchange bases as Free of Cost (FOC) under warranty.

v) Technical Support services should include resolution of complaints related to equipment.

vi) The drivers/applications support CD/media must be provided for hardware equipment compatible with the OS respectively (if any)

vii) Hardware devices having end of life must be communicated, moreover, nearly end of life hardware devices will not be acceptable.

viii) Vender will responsible for all types of IT equipment being delivered.

Note: *Vendor is solely responsible to provide the support services for the offered product even the support for the same product would have been discontinued by the OEM*

WARRANTY/ GUARANTEE

i. The successful bidder shall provide warranty/guarantee as specified in detailed specifications against each hardware item.

ii. The warranty period will start from the date of supplies received.

iii. The qualified bidder must warranty the IT Equipment and ensure availability of Technical support services as informed through electronic & non-electronic means. Each and every complaint should be completely responded by the competent resource of the firm and visit on-site within24 hours of its notification.

iv. If any bidder fails to rectify the problem in the provided equipment during warranty period due to any reason, FEDERAL OMBUDSMAN SECRETARIAT FOR PROTECTION AGAINST HARASSMENT (FOSPAH) will be authorized to repair or replace the faulty equipment/component thereof and forfeit the Bank Guarantee/Insurance Guarantee retained value.

v. The security deposit for warranty and guarantee will be released after expiry of the warranty period.

(SIGNATURE & SEAL OF BIDDER)

Form "A”

FINANCIAL PROPOSAL FOR PURCHASE OF IT EQUIPMENTS/PLANT & MACHINERY

Sr. No	Name of Items	Required Specifications	Specification of item being Offered by Firm	QTY	Unit Price without GST	GST	Total Unit Price with GST	Total Bid Cost
1.	**Laptop-I**	**HP, DELL, Lenovo, Acer or Equivalent** **Processor:** Intel Core i7, 14th Generation minimum **RAM:** 16GB DDR-5 or above **Hard Drive:** 1TB SSD (M2) NVMe or above **Screen size:** 13 inches or above, Full HD (1920 x 1080) IPS **Dedicated/External Graphics Card:** NVIDIA GeForce RTX or equivalent 4GB VRAM (GPU) **Operating System:** Licensed Microsoft Windows 11 Pro 64-bit **Warranty:** 1 Year official & local warranty (Must be verifiable online)		01				
2.	**Laptop-II**	**HP, DELL, Lenovo, Acer or Equivalent** **Must be a Pro/Business Series Laptop**		06				

		Processor: Intel Core Ultra 5, 14th Generation minimum **RAM:** 8GB DDR-5 or above **Hard Drive:** 512 GB SSD (M2) NVMe or above **Screen size:** 13 inches or above **Camera:** Integrated 720p HD **Wi-Fi & Bluetooth:** Wi-Fi 6E & BT ver. 5.3 **Operating System:** Licensed Microsoft Windows 11 Pro 64-bit **Warranty:** 1 Year official & local warranty (Must be verifiable online)						
3.	**Desktop Computer-I**	**HP, DELL, Lenovo, Acer or Equivalent** **Desktop (Tower Form):** **Processor:** Intel Core i7, Minimum 14th Generation **RAM:** 16GB DDR-5 or above **Dedicated/External Graphics Card:** 4GB GPU **Hard Drive:** 1TB SSD NVMe (M2) or above **Wireless & Connectivity:** Wi-Fi 6/6E & Bluetooth **Operating system:** Licensed Microsoft Windows 11 Pro 64-bit **LED monitor:** **Monitor size:** Pro Series 23.8 inches or above		01				

		Native Resolution: FHD (1920 x 1080) **Panel Type:** IPS **Connectivity (Interfaces):** HDMI, DisplayPort, VGA, USB, USB-C **Accessories:** Wireless Keyboard and Mouse, UHD 4K Pro Webcam **Warranty:** 1 Year official & local warranty (Must be verifiable online)						
4.	**Desktop Computer-II**	**HP, DELL, Lenovo, Acer or Equivalent** **Processor:** Intel Core i5, 13th Generation or higher **RAM:** 8GB DDR-5 or above **Hard Drive:** 512GB SSD NVMe (M2) or above **LED Monitor:** 20 inches or above. **Accessories:** Same brand Wired Keyboard & Mouse **Wireless & Connectivity:** Wi-Fi 6/6E & Bluetooth **Operating System:** Licensed Microsoft Windows 11 Pro 64-bit **Warranty:** 1 Year official & local warranty (Must be verifiable online)		07				
5.	**Heavy Duty Scanner**	**HP or Equivalent** **Scanner type:** Flatbed and ADF both **Digital sending standard features:** Scan to e-mail; Save to USB drive		01				

		Resolution: Up to 600 ppi **Duty cycle (daily):** 20,000 pages **Control panel:** Touchscreen; Virtual and Physical Keyboard **Maximum document scan size:** 11.7 x 17 in; Up to 11.7 x 34 in (long scan size) **Scan Speed (ADF):** Up to 120 ppm/240 ipm **ADF capacity:** 200 sheets **One-pass duplex scanning** **Scan file format:** PDF, JPEG, TIFF, MTIFF, XPS, PDF/A, TEXT (OCR), Unicode TEXT (OCR), RTF (OCR), Searchable PDF (OCR), Searchable PDF/A (OCR), HTML (OCR), CSV (OCR); **Image scaling or enlargement range:** 25 to 400% **Media size (ADF):** A3, Ledger, B4-JIS, A4, B5-JIS, A5, B6-JIS, A6 **Connectivity:** 10/100/1000 Ethernet (built-in Gigabit Ethernet); Hi-Speed USB Host **Warranty:** 1 Year official & local warranty (Must be verifiable online)						
6.	**Standard Scanner**	**HP or Equivalent** **Recommended daily duty cycle:** 4000 pages		03				

		Scan resolution, optical: Up to 600 dpi **Scan Size:** 8.5 x 122 in **Scan Speed:** Up to 40 ppm/80 ipm **Control panel:** Color touchscreen **ADF Capacity:** 50 pages **One-pass duplex scanning** **Connectivity:** Ethernet 10/100 Base-T, USB 3.0, Wi-Fi 802.11 b/g/n, Wi-Fi Direct **Scan file format:** For text and images: PDF, PDF/A, Encrypted PDF, JPEG, PNG, BMP, TIFF, Word, Excel, PowerPoint, Text (.txt), Rich Text (.rtf) and Searchable PDF **Warranty:** 1 Year official & local warranty (Must be verifiable online)						
7.	**Heavy Duty Multifunction Printer**	**HP or Equivalent** **Functions:** Print, Copy, Scan **Print speed black (A4):** Up to 45 ppm (default); Up to 52 ppm (Max High Speed) **Resolution (black):** Up to 1200 x 1200 dpi **Paper Size:** Letter; A4; Legal; Envelopes **Display:** Color touchscreen, Pull-out keyboard (physical)		02				

		Duplex printing: Automatic (standard) **Duty cycle (monthly, A4):** Up to 150,000 pages **Print technology:** Laser **Paper Storage:** Tray 1 (multipurpose): 100 sheets, Trays 2: 550 sheets **ADF capacity:** 100 sheets, Single-pass duplex ADF scanning **Connectivity:** Hi-Speed USB; Gigabit Ethernet; **Mobile printing capability:** Yes **Warranty:** 1 Year official & local warranty (Must be verifiable online) *** Consumable supplies(toner) must be available easily and at an affordable price**						
8.	**Heavy Duty Copier (Photocopy Machine)**	**Copier Type:** A3 Monochrome Laser Multifunctional, Office Copier, Floor-standing (trolley included) **Core Functions:** Print, Copy, Scan, Send, Store **Control Panel:** Color touch panel **Hard Disk drive:** 250 GB or above **Print/Copy speed:** Up to 45ppm (A4), Up to 32ppm (A4R), Up to 22ppm (A3) **Scan Speed:** Single Pass DADF (1-sided Scanning:		01				

		135ipm max, 2-sided Scanning: 270ipm max) **Print resolution:** up to 1200 x 1200 dpi **Copy resolution:** 600 x 600 dpi **Supported media sizes (Multi-purpose tray):** A3, A4, A4R, A5, A5R, A6R, B4, B5, B5R **DADF:** Duplexing Automatic Document Feeder **Document Feeder Paper Capacity:** Single Pass DADF (up to 200 sheets max) **Toner Impressions B/W:** 40,000 or above Impressions **Paper Supply Capacity (A4):** Standard 1,200 sheets (100-sheet Multi-purpose tray x 1, 550-sheet cassette x 2) Maximum: 6,350 sheets **Paper Output Capacity (A4, 80 gsm):** Standard 250 Sheets**,** Maximum: 3,350 Sheets **Connectivity:** 1000Base-T/100Base-TX/10Base-T, Wireless LAN (IEEE 802.11 b/g/n), 1 x USB 2.0, 1 x USB 3.0 **Printing from mobile and cloud:** AirPrint, Mopria, Google Cloud Print **Warranty:** Standard, 1 Year						

		*** Consumable supplies(toner) must be available easily and at an affordable price**						
9.	**Color PVC Printer**	**Print Method:** Direct-To-Card Dye Sublimation, Thermal Transfer (Dual Sided) **Printing Speed:** 1000 cards per hour monochrome, YMCKO single sided 230 cards per hour & YMCKOK Dual Sided 170 cards or higher **Hopper Capacity:** Input 100 Cards, Output 100 cards **Print Resolution:** 300×600 dpi (color), 300x1200 dpi (monochrome) **Card type (CR-80):** PVC cards, PET cards, ABS cards, and rewritable cards **Card thickness:** (1.25 mm / 50 mil) Max **Interface:** USB 3.0 and Ethernet **Accessories:** 100 blank PVC cards and one original YMCKO ribbon (300 prints capacity) *** The bidder is required to submit a manufacturer's authorization letter.** **Warranty:** 1-year standard manufacturer's warranty.		01				
10	**Wireless Access Point**	**Cisco, Huawei, TP-Link or Equivalent** **Wi-Fi Standards:** Tri-Band, 6-Stream, WiFi 6E Router,		02				

		Wi-Fi speeds up to 5400 Mbps **WiFi Speed:** 6 GHz band, 160 MHz Channel **Extensive WiFi Coverage** **Warranty:** Standard, 1 Year						
11	**Wireless Access Controller**	**Cisco, Huawei, TP-Link or Equivalent** **Ports:** 4 Gbps or above **Forwarding Capability:** 10 Gbit/s **Number of Managed APs:** 512 **Maximum Number of Access Users:** 4096 **Ducting, cabling, and configuration are included** (bidders may visit the office to assess the actual requirements) **Warranty:** Standard, 1 Year		02				
12	**Smartphones for FOSPAH's Helpline**	**Operating System:** Android 15 or above **2G Band:** SIM1: GSM 850 / 900 / 1800 / 1900 **SIM2:** GSM 850 / 900 / 1800 / 1900 **4G Band:** LTE band 1(2100), 5(850), 8(900), 40(2300) **CPU:** Octa-core (2 x 1.8 GHz Cortex-A75 + 6 x 1.8 GHz Cortex-A55) **Camera:** (Main): 50 MP, LED Flash, (Front): 5 MP		06				

		Technology: IPS LCD Capacitive Touchscreen **Size:** 6 Inches or above **Resolution:** 720 x 1608 Pixels or above **Storage:** 128GB Built-in or above **RAM:** 6GB Built-in or above **WLAN:** Wi-Fi 802.11 a/b/g/n/ac, dual-band **Bluetooth:** v5.2 with A2DP **USB:** Type-C 2.0, OTG **Capacity:** Li-ion 5500 mAh or above with Fast charging 40W or above **Warranty:** Standard, 1 Year						
Requirements (Plant & Machinery)								
13	**UPS**	**UPS:** 3 KVA Homage/Apollo/Winar/Solar or equivalent **Two Dry Batteries (02):** 2 x 200AH Exide/AGS/Phoenix/Volta or equivalent *** Complete installation, including ducting, cabling, and configuration, is included. (**Bidders may visit the office to assess the actual requirements) **Warranty:** 1 Year		03				

14	**Smart LED TV**	**TCL/Haier or equivalent** **Type:** Google Android TV-LED FHD **Size:** 55 inches or above **Resolution:** 4K **OS:** Android 15 or Above **Connectivity:** Bluetooth 5.0, Wifi 6E, USB, Ethernet, HDMI, Built-in Google/Chromecast **Speaker Type:** Integrated speakers **Wall Mount included** *** Complete installation, including ducting, cabling, and configuration, is included. (**Bidders may visit the office to assess the actual requirements) **Warranty:** Standard, 1 Year		01				
15	**Refrigerator**	**Dawlance/Haier or equivalent** **Type:** Refrigerator **Series:** Two-door **Total Capacity:** 240 Liters or above **Invertor Technology** **Warranty:** Standard (Compressor 10 Years), Electronics Parts (03 Years), Parts (01 Year)		03				
16	**Air Conditioner DC-Inverter (1.5 Ton)**	**Gree/Dawlance/Haier/TCL or equivalent**		05				

		DC inverter technology, particularly T3 compressor Wall-mounted (Inverter): 1.5 Ton *** Complete installation, including ducting, cabling, and configuration, is included. (**Bidders may visit the office to assess the actual requirements) **Warranty:** Standard, 1 Year						
17	**Floor Standing Air-Conditioner,** **(Chillers) (2 Ton) DC Inverter**	**Gree/Dawlance/Haier/TCL or equivalent** **DC inverter technology, particularly T3 compressor** **Floor Standing** (Inverter)**, 2 ton** *** Complete installation, including ducting, cabling, and configuration, is included. (**Bidders may visit the office to assess the actual requirements) **Warranty:** Standard, 1 Year		02				
18	**Bracket Fan**	**GFC/PakFan/Royal Fan or equivalent** Radius: 16 inches, Copper wire motor *** Complete installation, including ducting, cabling, and configuration, is included. (**Bidders may		05				

		visit the office to assess the actual requirements) **Warranty:** 1 Year							
19	**Instant Electric Geyser**	**Nasgas/Canon/Super Asia/Boss** **Tank capacity:** 15 liters **Overheating Protection**: Automatically prevents overheating for added safety *** Complete installation, including ducting, cabling, and configuration, is included. (**Bidders may visit the office to assess the actual requirements) **Warranty:** Standard, 1 Year		11					
Video Conferencing System (Head Office)									
20	**Camera Unit** **(Workplace Harassment & Property Rights Court)**	• Dual-eye 4K camera • 4K video at 30 frames per second • Auto Framing, Speaker Tracking, and Presenter Tracking • 12x Optical Zoom, 90° Wide Field of View (FoV) • Mechanical Pan, Tilt, and Zoom • PTZ control by remote control or camera control plug-in		02					

		• Audio integration • Support USB, HDMI, and VCH transmission • Wall Bracket and Accessories *** The bidder is required to submit a manufacturer's authorization letter.** • **Warranty:** Standard, 1 Year						
21	**AV Hub (Audio-Video Hub)**	• Central device to connect and manage multiple audio and video inputs • Multi-camera Layout • Support up to 8 microphones • Audio & Video Processing Capability • Support up to 9 x Dual-eye 4K cameras • Connectivity: 2 x USB-A Port, 1 x USB-B Port, 1 x Codec Port, 7 x VCH Port (RJ-45), 1 x RCA in/out Port, 1 x 6.3mm Line in Port, 1 x 6.3mm Line out Port, 1 x Power Supply Port *** The bidder is required to submit a manufacturer's authorization letter.**		01				

		• **Warranty:** Standard, 1 Year						
22	**Microphone Unit** **(Workplace Harassment & Property Rights Court)**	• HD Audio support • Full Duplex Technology • Acoustic Echo Canceling • Noise Proof Technology • 6m radius voice pickup range • Muting the microphone with touchpad *** The bidder is required to submit a manufacturer's authorization letter.** • **Warranty:** Standard, 1 Year		05				
23	**Speaker Unit** **(Workplace Harassment & Property Rights Court)**	**Audio Output:** • Stereo speakers • Frequency response: 100Hz-20KHz • Speaker volume: 89dB SPL @1W • Sensitivity: 89+/-2dB SPL • Root Mean Square (RMS): 10W **Audio Input:** • 1 x (RJ45), PoE support • 1 x 3.5mm Line-in **Interfaces:**		04				

		• Built-in Bluetooth • Power Input: Both through Power Adapter and PoE support **Accessories:** • 3m audio cable (3.5mm) • Wall Mount Bracket *** The bidder is required to submit a manufacturer's authorization letter.** **Warranty:** Standard, 1 Year							
24	**Video Conferencing Setup for Ombudsperson Office (All-in-one USB video bar)**	**Camera** • 20MP or above camera • 133° or above wide-angle lens • 8x e-PTZ camera • Electric lens cap • Camera presets **Audio** • Built-in microphone • Support extension mic • Built-in high-fidelity speaker • Noise Proof Technology • Beamforming directed voice pickup technology • Full-duplex • Echo cancellation **AI Technologies**		01					

		• Auto Framing, Speaker Tracking **Connectivity** • USB3.0 Type-B port • USB2.0 Type-A port • microphone port (RJ-45) • 3.5mm Line-in port • 1 x Power port • 1 x Security lock slot • 1 x Reset slot • Built-in Wi-Fi, remote device management • Applicable to most popular video conferencing Platforms *** The bidder is required to submit a manufacturer's authorization letter.** **Warranty:** Standard, 1 Year						
25	**Layer 2 Gigabit Network Switch with Integrated PoE Injection** **(Workplace Harassment & Property Rights Court)**	• Unmanaged Desktop Switch • 8× 10/100/1000Base-T ports with 802.3af/at PoE provisioning (max 120W budget) • Support VLAN tagging, QoS, storm control, IGMP snooping, IEEE 802.1p-based prioritization, auto MDI/MDIX and 4K MAC address table • Rack/wall-mountable		02				

		- **Warranty:** Standard, 1 Year						
26	**USB CABLE (10 Meters)** **(Workplace Harassment & Property Rights Court)**	- USB 3.0 shielded Type-B to A cable (UVC protocol grade) - 5Gbps bandwidth - Nickel-plated connectors - Triple EMI layer shielding - length: 10 meters - compliant with USB-IF Rev 1.2. - Certified for VC applications		03				
27	**UTP CAT6 Cable** **(Workplace Harassment & Property Rights Court)**	Length: 100 meters Installation (Wiring/Ducting), Testing & Training included		01				
Requirements to Set Up and Operate E-Filing System								
28	**Next Generation Firewall**	**General Requirements** 1. The proposed NGFW should be the leader in the latest Gartner Magic Quadrant for Enterprise Network Firewalls for more than 10 years. 2. The proposed NGFW should be ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, FedRAMP, Germany		01				

		C5, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSfC, USGV6, ICSA and NEBS certified 3. The proposed NGFW should require no reboot for checking and installing security updates 4. The proposed NGFW should have integrated reporting capabilities requiring no additional hardware to generate reports 5. The proposed NGFW should identify applications regardless of port, SSL/SSH encryption, or evasive techniques employed 6. The proposed NGFW should categorize unidentified applications for policy control, threat forensics, or application identification technology development 7. The proposed NGFW should be a natively engineered security solution (Not an application control blade with underlying stateful inspection firewall) 8. The proposed NGFW should be a natively engineered appliance with a single-pass						

		parallel processing architecture for traffic processing 9. The proposed NGFW should have integrated traffic shaping functionality (QoS) based on source/destination IP, port, protocol, and application 10. The proposed NGFW must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability 11. The proposed NGFW should control access and enforce policies for websites and applications, including SaaS applications 12. The proposed NGFW should have a single OS across all form factors 13. The proposed NGFW should support creating security policies to prevent credential theft 14. The proposed NGFW should support enforcing multi-factor authentication to internal applications 15. The proposed NGFW should support an unfettered open API without a paywall (subscription) to access						

		Dev toolkit, Tools and Scripts and samples 16. The proposed NGFW should support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed 17. The proposed NGFW must provide visibility and the ability to restrict applications using non-standard ports in a single security policy rule 18. The proposed NGFW must be able to tag objects to enable dynamic enforcement of policy no matter any changes to IP, area, or direction traffic originates from with no need to recommit policy 19. The proposed NGFW must be able to provide Machine Learning algorithms for advanced protections directly from the NGFW with no external connections needed 20. The proposed NGFW should grant easy OS updates without the need of certain combinations for hotfixes or patches to be in place						

		21. The proposed NGFW should have a feature of holding multiple OS images to support resilience and easy roll-backs during the version upgrades 22. The proposed NGFW should support enabling any new security offering without impacting the performance of the traffic flowing through it 23. The proposed NGFW should have a feature of identifying what applications are hitting the security policies and migrating these policies into application-based policies 24. The proposed NGFW should offer redundant AC power supplies **Architecture, Physical & Performance Specifications** 1. The proposed NGFW should deliver 2.6 Gbps of documented firewall throughput (Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions) 2. The proposed NGFW should deliver 1.2 Gbps of documented threat prevention throughput (Threat Prevention						

		throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions) 3. The proposed NGFW should deliver 1.1 Gbps or above of IPsec VPN throughput (IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled) 4. The proposed NGFW should support 200,000 Max sessions 5. The proposed NGFW should support 34,000 new connections per second (measured with application-override utilizing 1byte HTTP transactions) 6. The proposed NGFW should support the addition of virtual systems for future expansion 7. The proposed NGFW must support minimum of 8 x 1G RJ45 8. The proposed NGFW should support 1 x 10/100/1000 out-of-band management port ,1 x RJ45 console port , 2 x USB port 9. The proposed NGFW should support						

		Active/Active, Active/ Passive & Clustering deployments 10. The proposed NGFW should support state full session maintenance in the event of a fail-over to a standby unit 11. The proposed NGFW should support the High Availability feature for either NAT/Route or transparent mode 12. The proposed NGFW should support multiple heartbeat links 13. The proposed NGFW should support L3, L2, transparent and tap mode deployments **Security Policy Control features** 1. The proposed NGFW should support creating security policies based on Layer 7 applications irrelevant to the TCP/UDP port number (non-profile-based application control) 2. The proposed NGFW should support the management of unknown traffic (unidentified applications) through security policies 3. The proposed NGFW should have a built-in security policies optimization tool which facilitates converting						

		legacy Layer 4 port-based security policies to Layer 7 application-based ones 4. The proposed NGFW should support enforcing security policies based on a schedule 5. The proposed NGFW should simplify rule use tracking via a timestamp for the most recent rule match, a timestamp for the first rule match, and a rule hit counter **Advanced Threat Prevention Features** 1. The proposed NGFW should protects networks by providing multiple layers of prevention, confronting threats at each phase of an attack 2. The proposed NGFW should detect and block threats on any and all ports instead of invoking signatures based on a limited set of predefined ports 3. The proposed NGFW should benefit from other cloud-delivered security subscriptions for daily updates that stops exploits, malware, malicious URLs, command and control (C2), and spyware						

		4. The proposed NGFW should provide protections against unknown threats instantly by embedding ML in the core of the firewall to provide inline signatureless attack prevention 5. The proposed NGFW should utilize Inline malware protection—through signatures based on payload, not hash 6. The proposed NGFW should continuously collect telemetry to enable data-intensive ML processes to automatically compute and recommend policy changes 7. The proposed NGFW should use cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW 8. The proposed NGFW should leverage heuristic-based analysis detects anomalous packet and traffic patterns, such as port scans, host sweeps, and denial-of-service (DoS) attacks 9. The proposed NGFW should support creating custom signatures, which allows tailoring intrusion prevention capabilities to a							

		network's unique needs 10. The proposed NGFW should support other attack protection capabilities, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect against evasion and obfuscation techniques 11. The proposed NGFW should employ natively integrated defensive technologies to ensure that, when a threat evades one technology, another catches it 12. The proposed NGFW should inspect and classify traffic as well as detect and block both malware and vulnerability exploits in a single pass 13. The proposed NGFW should comb each packet as it passes through the platform, looking closely at byte sequences within both the packet header and payload 14. The proposed NGFW should analyze the context provided by the arrival order and sequence of multiple packets to catch and prevent evasion techniques						

		15. The proposed NGFW should support protocol decoder-based analysis 16. The proposed NGFW should provide protocol anomaly-based protection 17. The proposed NGFW should leverage inline, stream-based detection and prevention of malware hidden within compressed files and web content 18. The proposed NGFW should provide protections against payloads hidden within common file types, such as Office/Microsoft 365 documents and PDFs 19. The proposed NGFW should enable the correlation of a series of related threat events (e.g., from Threat Prevention logs) that, when combined, indicate a likely attack 20. The proposed NGFW should have an option of configuring exception 21. The proposed NGFW should be able to detect & prevent the malware by scanning different file types 22. The proposed NGFW should be able to identify malwares						

		coming from incoming files and malwares downloaded from Internet 23. The proposed NGFW should provide an option to create custom signature for applications 24. The proposed NGFW should have all major applications signatures and it should able to understand well known application like P2P and voice without any dependency on the port 25. The proposed NGFW should enforce inline deep learning for real-time enforcement for new and unknown command and control 26. The proposed NGFW machine learning and deep learning models should be aligned to key protocols, such as SSL, HTTP, unknown UDP, and unknown TCP 27. The proposed NGFW should use ML-based analysis to identify advanced DNS-based threats 28. The proposed NGFW should utilize a cloud-based database which contains tens of millions of known malicious domains, enabling the blocking of phishing,						

		malware, and other high-risk categories 29. The proposed NGFW should provide threat reporting capabilities that allow full visibility into DNS traffic, along with the full DNS context around security events and traffic trends over time 30. The proposed NGFW should enable forging a response to a DNS query for a known malicious domain and cause that malicious domain name to resolve to a definable IP address given to the client to identify infected hosts 31. The proposed NGFW should allow defining separate policy actions as well as a log severity level for a specific signature type 32. The proposed NGFW should identify the use of DGAs, which generates random domains on the fly for malware to use as a way to call back to a C2 server 33. The proposed NGFW should identify DGA (Domain Generation Algorithms) domains based on dictionary words 34. The proposed NGFW should prevent the use						

		of DNS tunneling, which exploits the DNS protocol to tunnel malware and other data through a client-server model 35. The proposed NGFW should disrupt ultra-low/slow DNS tunnels that spread tunneled data and exploits across multiple domains and use very slow rates to evade detection, stealing data or sending additional malicious payloads into your network 36. The proposed NGFW should leverage predictive analytics that protect users from connecting to domains that were reserved and left dormant for months before use by malicious actors 37. The proposed NGFW should prevent fast flux domains 38. The proposed NGFW should protect against domains surreptitiously added to hacked DNS zones of reputable domains 39. The proposed NGFW should prevent DNS rebinding attacks, which can be used to move laterally and attack services inside the corporate network from the internet						

		40. The proposed NGFW should prevent dangling DNS attacks 41. The proposed NGFW should prevent attackers from directing users to malicious domains with the use of a wildcard DNS record 42. The proposed NGFW should prevent techniques that exploit DNS protocol to tunnel malicious payloads into networks 43. The proposed NGFW should protect users from connecting to domains that can be used to launch DDoS attacks 44. The proposed NGFW should support traffic static analysis 45. The proposed NGFW should support traffic dynamic analysis 46. The proposed NGFW should support advanced file analysis with URL crawling to prevent multistage, multihop attacks 47. The proposed NGFW analysis environment should replicate macOS, Android, Windows XP/7/10, and Linux 48. The proposed NGFW file analysis should support PE files (EXE, DLL, and others), all						

		Microsoft Office file types, Mac OS X files, Linux (ELF) files, Android Package Kit (APK) files, Adobe Flash and PDF files, archive (RAR and 7-Zip) files, script (BAT, JS, VBS, PS1, Shell script, and HTA) files, analysis of links within email messages, and encrypted (TLS/SSL) files 49. The proposed NGFW support protocols should be SMTP, POP3, SMB, FTP, IMAP, HTTP, and HTTPS 50. The proposed NGFW should generate signatures based on the malware payload of the sample and tested for accuracy and safety 51. The proposed NGFW should provide protection updates for unknown malware within seconds **Advanced URL Filtering** 1. The proposed NGFW should possess a patented inline real-time web threat prevention capability which uses cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time						

		2. The proposed NGFW machine-learning models should get retrained frequently, ensuring protection against new and evolving never before-seen threats (e.g., phishing, exploits, fraud, C2) 3. The proposed NGFW should protects against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding 4. The proposed NGFW URL database should maintain hundreds of millions of known malicious and benign URLs categorized through a combination of static, dynamic, machine learning, and human analysis 5. The proposed NGFW should be allow classifying websites based on site content, features, and safety, and includes more than 70 benign and malicious content categories 6. The proposed NGFW should support risk rating which scores URLs on a variety of factors to determine risk 7. The proposed NGFW should have multi-category support which categorizes a URL with						

		up to four categories, allowing for flexible policy and the creation of custom categories 8. The proposed NGFW should detect and prevent credential theft by controlling sites to which users can submit corporate credentials based on the site’s URL category 9. The proposed NGFW should se ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts 10. The proposed NGFW allow designating multiple policy action types based on URL categories or criteria 11. The proposed NGFW should apply URL filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies 12. The proposed NGFW should apply URL filtering policies when end users attempt to view the cached results of web searches and internet archives 13. The proposed NGFW should prevent inappropriate content						

		from appearing in users’ search results 14. The proposed NGFW should enable administrators to notify users of a violation using a custom block page 15. The proposed NGFW should support crawling and analysis in 41 languages **User Identification & Authentication Features** 1. The proposed NGFW should support identifying user-id by integrating with Active Directory through WinRM and WMI 2. The proposed NGFW should support identifying user-id by integrating with Exchange through WinRM and WMI 3. The proposed NGFW should support identifying user-id by running as sy slog receiver 4. The proposed NGFW should support identifying user-id by Integrating through XML APIs with Third Party solutions 5. The proposed NGFW should support identifying user-id through captive portal						

		6. The proposed NGFW should support Identifying user-id in terminal servers 7. The proposed NGFW should support identifying user-id by running an agent at user machines 8. The proposed NGFW should have direct Multi-Factor Authentication integration with RSA, Okta, PingID and Duo 9. The proposed NGFW should support SSO authentication 10. The proposed NGFW should support multiple server profiles like SAML 2.0, Radius, LDAP, Tacacs+, and Kerberos. **Advanced Mobility & Host Information Profiling Features** 1. The proposed NGFW should offer a remote user VPN agent for Windows, MAC, Linux, Chrome, iOS, and Android 2. The proposed NGFW should support app-Level VPN for iOS and Android devices 3. The proposed NGFW should have support portal based and clientless SSL VPN						

		4. The proposed NGFW should support MFA 5. The proposed NGFW should offer a host information check feature by collecting & reporting device information & attributes. Host Information Profiling attributes based on Managed/Unmanaged certificates status, OS type, Client version, Host name, Host ID, Serial number, Mobile model, Phone number, Root/Jailbroken status, Passcode presence, Installed Applications, Patch presence & status, Firewall agent presence & status, Antimalware agent presence & status, Disk backup agent presence & status, Disk encryption agent presence & status, DLP agent presence & status, process list presence & status, registry key presence & status and Plist presence & status 6. The proposed NGFW should support enforcing security policies based on device/host information profiles 7. The proposed NGFW should support the integration with Third Party MDM solutions							

		like AirWatch or MobileIron 8. The proposed NGFW should support split tunneling based on IP addresses, domains and applications 9. The proposed NGFW should support VPN authentication override using cookies 10. The proposed NGFW should support the exclusion of video traffic from main remote user VPN tunnel 11. The proposed NGFW should support trusted root certificates push to remote VPN user devices to help enable features like SSL offload 12. The proposed NGFW should support VPN gateway selection criteria based on source user-id, region, OS and IP address **Management, Logging & Reporting Features** 1. The proposed NGFW should offer a Command Line Interface (CLI) 2. The proposed NGFW should offer a built-in web interface, non Java base (GUI) 3. The proposed NGFW should support XML						

		Rest API based management 4. The proposed NGFW should have a commit-based configuration management 5. The proposed NGFW should support config-audit by comparing running config against candidate config 6. The proposed NGFW should offer an interactive graphical summary around the applications, users, URLs, threats, and content traversing the network 7. The proposed NGFW should offer a customized graph-based network activity for applications using non-standard ports 8. The proposed NGFW should offer a customized graph-based blocked activities which includes blocked applications activity, blocked users activity, blocked content activity, blocked threats activity, and security policies blocking activity 9. The proposed NGFW should offer a customized graph-based tunnel activities including tunnel ID/Tag, tunnel application usage, tunnel user activity, and tunnel ip							

		source/destination activity 10. The proposed NGFW should support custom reporting with the ability to generate a report per user, user group and application 11. The proposed NGFW should support exporting reports to PDF and sending reports by email 12. The proposed NGFW should have a dedicated SaaS applications usage report 13. The proposed NGFW should have dedicated log sets for traffic, threats, URL filtering, data filtering, file control, user id mapping, authentication, configuration, system and alarms 14. The proposed NGFW should support custom admin roles 15. The proposed NGFW should allow administrators to work directly on the appliance, and make configuration changes as needed, without having to log in to a central manager 16. The proposed NGFW should allow central administrators to						

		monitor and view the changes made by local administrators 17. The proposed NGFW management should be done directly through the appliance without the need of installing any clients or virtual machines 18. The proposed NGFW should offer the ability to choose which firewall administrator’s configuration changes to be committed on the firewalls 19. 1The proposed NGFW should offer the ability to quickly roll back changes from specific users and restore configurations 20. Three (03) years license: 1. Advance Threat prevention subscription. 2. Sandboxing subscription. 3. Advanced URL Filtering Subscription. 4. DNS Security subscription. 5. SD-WAN						
29	**Network Data Switch (L2) 48x Gigabit Ports**	**General requirements** • Switch must be covered with official warranty of the manufacturer on the territory of Pakistan		01				

		for a period of not less than 1 years • The switch must be equipped with 10/100/1000BaseT ports, not less than 48 • The switch must be equipped with SFP ports, not less than 8 x 1/10Gb SFP+ uplink ports (includes 2 x Stacking ports) • MACsec-capable • The switch must support fabric technology • The switch must be equipped with out-of-band 10/100BaseT Ethernet port for management • The switch must be able to mount in 19" Rack. Required rackmount kit must be included. **Performance** • The switching bandwidth must be not less than 256 Gbps • The switch should have non-blocking architecture. All ports must operate on highest possible speed simultaneously • The maximum number of stored MAC addresses in						

		the switching table the switch shall be not less than 32,000 • The routing table of the switch must store not less 16,000 IPv4 routes • The switch must support 6,000 or more Multicast groups **Stacking** • The switch must support stacking with other families of switches from the same manufacturer and stack bandwidth must be not less than 40Gbps • The failure of any switch in the stack should not cause stack outage more than 20ms. • The switch must support the joint failover configuration with another identical switch to connected devices can use the mechanism for combining multiple physical channels (LAG) to two switches with active simultaneous use of all channels; the recovery Time in case of any link failure between switches should not exceed 50ms.						

		• The failover configuration must be supported for two separate switches and two separate stacks of switches. **Ethernet L2** • The switch must support the IEEE family protocols: 802.3: 802.3, 802.3ae, 802.3ab, 802.3z. • The switch must support 802.1ad (Q-in-Q) and Selective Q-in-Q protocols • The switch mush support High Availability Network Protocols with 50ms recovery time in ring topology with RFC 3619 Ethernet Automatic Protection Switching. • The switch must support 802.1w, 802.1s, PVST+ protocols • The switch must support Link Aggregation Group (LAG). Number of ports in one LAG must be not less than 8 • The switch must support the following mechanisms for traffic balancing in LAG: The combination of the						

		MAC addresses of source and destination; • The combination of IP addresses of source and destination; • The combination of IP addresses of source and destination, and numbers of TCP and UDP port numbers; • The combination of IPv6 source and destination and numbers of the protocols of the 4th layer of the OSI model. • The switch must support 802.1AS, 802.1Qav, 802.1Qat, 802.1BA **Routing IPv4/IPv6** • The switch must support Policy-based Routing • The switch must support BFD for static routing and dynamic routing protocols OSPFv2/OSPFv3 **L2/L3 Multicast** • Then switch must support Multicast VLAN registration (MVR) protocol						

		• The switch must support IGMPv1 / v2 / v3 protocols; • The switch must support protocols: IGMPv1 / v2 / v3 snooping (IGMPv1 / v2 / v3 snooping); • The switch must support the protocol PIM Snooping; **User authorization and QoS** • Each interface for connecting user devices must support at least 8-x hardware queues. • Access control lists that are configured on the switch port must operate at line speed available on port. • The switch must support the IEEE 802.1x protocol. • The switch should provide dynamic assignment of user access policies L2-L4 on ports **Management** • The switch must support standard SNMP versions 2c and 3, Syslog. • The switch must support NTP • Switch must support on Prem						

		management and cloud management **Warranty:** Standard, 1 Year or above							
30	**Network Data Switch (L2) 24x Gigabit Ports**	**General requirements** • Switch must be covered with official warranty of the manufacturer on the territory of Pakistan for a period of not less than 1 years • The switch must be equipped with 10/100/1000BaseT ports, not less than 24 • The switch must be equipped with SFP ports, not less than 8 x 1/10Gb SFP+ uplink ports (includes 2 x Stacking ports) • MACsec-capable • The switch must support fabric technology • The switch must be equipped with out-of-band 10/100BaseT Ethernet port for management • The switch must be able to mount in 19" Rack. Required rackmount kit must be included. **Performance** • The switching bandwidth must be		01					

		not less than 208 Gbps • The switch should have non-blocking architecture. All ports must operate on highest possible speed simultaneously • The maximum number of stored MAC addresses in the switching table the switch shall be not less than 32,000 • The routing table of the switch must store not less 16,000 IPv4 routes • The switch must support 6,000 or more Multicast groups **Stacking** • The switch must support stacking with other families of switches from the same manufacturer and stack bandwidth must be not less than 40Gbps • The failure of any switch in the stack should not cause stack outage more than 20ms. • The switch must support the joint failover configuration with another identical switch to connected						

		devices can use the mechanism for combining multiple physical channels (LAG) to two switches with active simultaneous use of all channels; the recovery Time in case of any link failure between switches should not exceed 50ms. • The failover configuration must be supported for two separate switches and two separate stacks of switches. **Ethernet L2** • The switch must support the IEEE family protocols: 802.3: 802.3, 802.3ae, 802.3ab, 802.3z. • The switch must support 802.1ad (Q-in-Q) and Selective Q-in-Q protocols • The switch mush support High Availability Network Protocols with 50ms recovery time in ring topology with RFC 3619 Ethernet Automatic Protection Switching. • The switch must support 802.1w, 802.1s, PVST+ protocols						

		• The switch must support Link Aggregation Group (LAG). Number of ports in one LAG must be not less than 8 • The switch must support the following mechanisms for traffic balancing in LAG: The combination of the MAC addresses of source and destination; • The combination of IP addresses of source and destination; • The combination of IP addresses of source and destination, and numbers of TCP and UDP port numbers; • The combination of IPv6 source and destination and numbers of the protocols of the 4th layer of the OSI model. • The switch must support 802.1AS, 802.1Qav, 802.1Qat, 802.1BA **Routing IPv4/IPv6** • The switch must support Policy-based Routing						

		• The switch must support BFD for static routing and dynamic routing protocols OSPFv2/OSPFv3 **L2/L3 Multicast** • The switch must support Multicast VLAN registration (MVR) protocol • The switch must support IGMPv1 / v2 / v3 protocols; • The switch must support protocols: IGMPv1 / v2 / v3 snooping (IGMPv1 / v2 / v3 snooping); • The switch must support the protocol PIM Snooping; **User authorization and QoS** • Each interface for connecting user devices must support at least 8-x hardware queues. • Access control lists that are configured on the switch port must operate at line speed available on port. • The switch must support the IEEE 802.1x protocol. • The switch should provide dynamic assignment of user						

		access policies L2-L4 on ports **Management** - The switch must support standard SNMP versions 2c and 3, Syslog. - The switch must support NTP - Switch must support both on-premises management and cloud management. **Warranty:** Standard, 1 Year or above						
31	**Data Rack for IT equipment, switches and other accessories**	**Server Rack:** 27U-Floor Standing 19” or larger. **Width:** 600mm **Depth:** 1000mm **Front and Back Mesh Door** **Side Panels removable** **Trays:** 1 x Fixed Tray, 1 x Sliding Tray, 4 x Cooling Fans **PDU:** 8 Ports Universal Multi-Socket Power Distribution Unit **Warranty:** Standard, 1 Year		01				
32	**Datacenter Network Renovation**	**CAT 6 Cable** - Cat 6 Cable, UTP, PVC, 4 pairs, 305 meter/ Box Gigabit original copper cable Category 6 U/UTP Cable		01				

		• Unshielded Category 6/Class E systems when installed with Cat-6 RJ45 Jacks. • Conductor Diameter: AWG 24 (Ø 0.525 +/- 0.015mm) • Insulation Diameter: PE Ø 0.95 +/- 0.05 mm • Cable assemblies: pairs • Sheath material: PVC **Mechanical Features:** • Maximum cable diameter (mm) 5.40 +/- 0.30 • Bending Radius (mm) • Dynamic (installation) / Static (installed) ≥ 8x outer diameter / ≥ 4x outer diameter • Temperature Range In service / Installation, Transport and Storage -20°C +60°C / 0°C +50°C **Standards Cables** • IEC 61156-5 ed. 2 • ANSI/TIA 568-C.2 • ISO/IEC11801 ed.2 **Fire Rating** • LSZH: IEC 60332-1 • PVC: IEC 60332-1						

		Patch Panel • 1U 19” panels must be available to take a minimum of 24 copper fully shuttered jacks. Other • connection densities must be available: • The panels must be designed for keystone fitting of the fully shuttered jacks/sockets. For efficiency of the termination and performance tool less terminate able keystone jacks must be used. • The copper panel panels must have cable management and tie down points (where required) for copper cable. Panels must have the facility to label each fully shuttered socket/jack. **CAT6 I/O** • RJ45 K6 Jack, Cat 6, UTP, Shuttered (tool-less termination), • Category 6/Class E system, fully compliant with Category 6 ISO/IEC, EN and TIA standards • for hardware performance,						

		confirmed by independent laboratory certifications (Delta, • GHMT). **The jacks must have the following features:** • Category 6 UTP • Keystone fixing; • Tool less assembly (mandatory) • Capable of being wired to both 568B and 568A • three cable entry points • Integral shutter/shuttered jack • Jacks must be reusable i.e it must support multiple terminations. **Applications** • IEEE 802.3 1GBASE-T • PoE – IEEE 802.3at **Standards** • ISO/ IEC 11801 Edition 2, Am 1-2 • ISO/ IEC 60603-7-5 • EN 50173-1 • ANSI/ TIA/ EIA-568-C.2-2009 • IEC 60512-99-001 **Faceplate**						

		• Single non-shuttered • U.K. Single Gang Faceplate, 1 port, w/o shutter. • 86 x 86 faceplate range can be loaded with Cat-6 UTP I/O to provide the following configurations: ◦ Single gang, 1 port ◦ Single gang, 2 ports **Patch Cord** • Patch cables must be available in either LSOH or PVC jackets. 100-Ohm RJ-45 copper patch cords shall be Category 6.						
Training Hall/Room (Audio Visual) requirements								
33	**Interactive Screen**	**Display:** • **Screen size:** 98 inches or above • **Resolution:** 4K UHD (3840 x 2160 or above) • **Panel Type:** IPS • **Number of Touch Points:** 20 Points in Android or higher and 40 Points in Windows. **Video Conferencing support:**		01				

		• **Camera:** Built-in Dual-48MP Camera, face tracking, Speaker-Tracking, Standard/ Normal view & Wide view. • **Microphone Array:** Built-in 12-Microphone Array or higher with AGC/ANR/AEC • **Speaker:** Built-in Speaker 20W x 2. **Built in Public Addressing System.** **Wireless casting support** with lifetime wireless casting software subscription. **Processor:** • Multicore (8 cores) 64-Bit processors (Built-in) • Intel Core i5 12th Generation or above (OPS) **Operating System:** • Android 13 or above (Built-in) • Windows 11 Pro Licensed version (OPS) **Memory:** • **RAM:** 8 GB (Built-in) • **Flash Memory/ROM:** 64 GB (Built-in) • **RAM:** 8 GB (OPS) • **SSD:** 256GB (OPS) **Connectivity:**						

		• **Wi-Fi:** Dual Wi-Fi 6 (2.4 GHz & 5 GHz) • **Bluetooth:** ver. 5.2 • **OPS:** Included **Accessories:** Wall-mounted Bracket and Rolling Stand **Warranty:** Standard, 1 Year * **Complete installation, including ducting, cabling, and configuration, is included. (**Bidders may visit the office to assess the actual requirements)						
34	**Portable Speaker**	**Type:** Portable speaker **Output power (W):** 100 watts or above **Dynamic frequency response range (Hz):** 50 Hz - 20k Hz @-6dB or above **Bluetooth frequency:** 2.4 GHz or above **Bluetooth version:** 4.1 or above **Battery:** Rechargeable **Maximum backup time (hrs):** 07 and above **Accessories:** 02 x Rechargeable Handheld Wireless Microphones, 01 x Rechargeable Lavalier Lapel Wireless Microphone **Warranty:** Standard, 1 Year		01				

Media and Communications Section Requirements								
35	**Microphone**	• Suitable for home-studio recording, podcasting, video conferencing, vocals, and instrument recording. • Delivers smooth and wide-spectrum frequency response. • Features two selectable polar patterns: Cardioid and Omnidirectional. • Supports 24-bit/48 kHz high-resolution audio. • Offers latency-free monitoring and a mute function. • Includes a 3m Type-C to USB cable, a 2m Type-C cable, and a durable desktop stand. • Must be compatible with Windows, Mac computers, and most Type-C devices. • **Warranty:** Standard, 1 Year		01				
36	**DSLR Camera**	**Camera Type:** • Digital Single-Lens Reflex (DSLR) Camera **Sensor:** • Type: CMOS Sensor • Size: Minimum APS-C or Full Frame		01				

		• Effective Resolution: 26.2 Megapixels or above **DIGIC 8 Image Processor** **Autofocus System** **Video Recording:** • Resolution: Full HD 1080p or 4K UHD at 30 fps or higher • Built-in microphone and external mic input **Equipped with a 2.36M-dot OLED electronic viewfinder.** **Connectivity:** • Wi-Fi, Bluetooth, or NFC support **Storage:** • Compatible with SD/SDHC/SDXC memory cards **Lens:** • Standard kit lens (e.g., 18–55mm) included **Battery:** • Rechargeable lithium-ion battery with charger included **Accessories:** • Camera bag **Warranty:** • 1-year standard manufacturer’s warranty						

(SIGNATURE & SEAL OF BIDDER)

DOCUMENTS CHECKLIST FOR VENDOR

S #	Documents	Attached (Please tick)
1.	Request Letter for Tender Documents	
2.	CNIC copy	
3.	Company Profile	
4.	Bid Security	
5.	Financial Proposal (bid offer on above format)	
6.	Vendor Details (NTN, GST certificates etc)	
7.	Bank A/c, IBAN, Mobile No. & Email Address.	

(SIGNATURE & SEAL OF BIDDER)