Alexandria International Container Terminal Company S.A.E

(Private free Zone Company)

Request for Proposal

For

IT Infrastructure Tender for National Operation Centre Start-up

Reference No. T/AICT/IT/02/2025

(Version 1.0)

March 2025

1 INTRODUCTION

1.1 Our work

Alexandria International Container Terminal Company S.A.E is a part of the Hutchison Port Holdings' (HPH) global network of container terminals. HPH is the leading independent port developer and operator in the world. In its short operating target, ALEXANDRIA INTERNATIONAL CONTAINER TERMINAL COMPANY red need to establish itself as the preferred terminal operator by achieving high levels of operating efficiency and customer satisfaction.

1.2 Purpose

Alexandria International Container Terminal Company S.A.E invites qualified vendors to submit their best competitive solutions to provide a comprehensive solution for deferent services and hardware to have excellent implementation and cover all technical requirement to achieve operation needs for National Operation Center (NOC) in Cairo.

1.3 PRE-QUALIFICATION CRITERIA

1- Bidder should confirm in their letterhead that OEM for the proposed projects is from Leader's quadrant of Gartner's report and should submit latest Gartner report.
2- The bidder should have successfully implemented IT infrastructure Projects for at least 3(three) domestic customer / organization during the last 3 (three) years from the Tender closing date.
3- the bidder provides an undertaking that the OEM shall provide Direct Premium support for the supplied hardware including system software.
4- All service requests for all projects should be received, managed, executed, and tracked to closure by the OEM or authorized representative's partner.
5- National Operation Center (NOC) reserves the right to accept or reject any bid or to annul the bidding process and reject all bids at any time prior to award of the Contract / Purchase Order without assigning any reason whatsoever and without thereby incurring any liability whatsoever to the affected Bidder(s). Mere submission of tender document shall not mean fulfilment of requirements of eligibility of the Bidder(s).
6- The bidder should Submit in all projects in this tender
7- The quantities mentioned in the tender is indicative, and the actual number may vary depending on the requirement. While placing the order, Alexandria International Container Terminal Company S.A.E may increase or decrease the quantities of items in the tender or request to deliver the items in patches according to the needs and the bidder shall be bound to supply the quantities of items so ordered.

8- Bidders must submit below documents.

a- Bidder's Profile, Experience of similar projects, OEM Partnership certificate, Declaration letter for not blacklisted by OEM and CV of the project manager and indicative CVs of onsite engineers.
b- The Bidder's confirmation for OEM listed as leaders on Gartner's Magic quadrant
c- Direct Premium Support undertaking from OEM which should be minimum of 24x7 remote support with maximum resolution time of Next Business Day (NBD).
d- Delivery plan & schedule.
e- Bill of material and quantity with OEM Product and Services Part No.
f- Completed technical specifications.
g- Product brochures and cross reference document pertaining to technical specification (as relevant).
h- 3 local references in Egypt with their use's cases (same scale).

2 VOIP PROJECT

2.1 PURPOSE OF THE PROJECT:

The purpose of this RFP is to invite technically and commercially competitive proposals from reputed manufacturers/authorized representatives for **VOIP solution**. The vendor engagement will involve Supply, Installing, Configuring, Testing, Implementing, and Commissioning of the new solution, as well as providing incident and product support as per Scope of work and Technical Specifications given in this RFP, at National Operation Center (NOC) Datacenter.

2.2 SCOPE of work

- The broad scope of work as detailed in this section refers to the Hardware and System software that is procured through this tender and used for Supply, Installing, Configuring, Testing, Implementing and Commissioning of the **VOIP solution** supporting over **100 concurrent calls**, including external, and inter-site communications at National Operation Center (NOC).

- The organization operates the following VoIP solutions:
  - Cisco Call Manager: Implemented at two sites.
  - Avaya IP Office: Implemented at one site.
- These sites will be integrated with National Operation Center (NOC) using a SIP trunk. The National Operation Center (NOC) will also be connected to Telecom Egypt for external call services.
- A cloud-based architecture is mandatory for the proposed VoIP system
- **Licensing Coverage**: The bidder/OEM must ensure that all necessary licenses for the VoIP solution are fully covered, including those required for integration with additional sites and Telecom Egypt.
- **Responsibility for Additional Licenses**: If any licenses needed to complete the solution are identified after the proposal is submitted, the bidder/OEM will be responsible for covering the costs of those additional licenses.
- **this scope of work shall include, but not be limited to, the following:**

2.2.1 GENERAL CONDITIONS

- The OEM shall be responsible for Design, Supply, Installation, Configuration, Testing and Commissioning of the **VOIP solution** in at National Operation Center (NOC).

- The OEM shall be doing the Project Management for the entire Project from commencement to final handing over for live use. The proposed solution must be supported for a period of 3 years as per RFP and National Operation Center (NOC) requirement.

- The OEM must prepare architecture design, optimize network to increase performance, documentation, and project plan as part of the implementation services.

- Installation and configuration of supplied hardware associated system software and system integration must be carried out by Bidder.

- Bidder should propose highly scalable solution. Solutions with limited scalability would not be acceptable to National Operation Center (NOC).
- The bidder must submit a detailed plan for implementation of the solution. The plan should include the full scope of the project as mentioned above. On acceptance of such plan by National Operation Center (NOC), the OEM is required to carry out the implementation, customization as applicable including supply, installation, and testing of solution etc. The OEM shall also handle all matters relating to the configuration and operation of the system including but not limited to application, system interfaces, documentation, user manual and training for the successful implementation of the system. The project plan update to be published bi-weekly till the project completion.
- The solution implemented should have high availability features to ensure that systems will be available at any time of the day.
- The Bidder/OEM shall be responsible for performing the necessary changes in the configuration required for Hardening and/or request directed by security team & audit team.
- The Bidder/OEM shall be responsible for firmware patches/bug, fixes BIOS upgrade and Version Upgrade of software.
- The Bidder/OEM shall be responsible for generation and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams and other reports etc. All such documents shall commence only after the same is approved by National Operation Center (NOC).
- The Bidder/OEM should provide a detailed project plan in terms of activity and phase-wise timelines (no. of days) required for executing the project with the details of deliverables and milestones including the delivery of Server components. The Bidder/OEM shall inform the name of the Project Manager who would be the single point of contact during the complete project implementation.
- The Bidder/OEM shall be responsible for installing / configuring of all patches / updates / upgrades required for the offered solution without any extra cost to National Operation Center (NOC) during the warranty period.
- All service requests for **VOIP solution** should be received, managed, executed, and tracked to closure by the OEM and not through Authorized Service Provider.
- The bidder shall Plan & Design the Architecture services from the OEM. The entire hardware and software supplied under this RFP must be installed and configured by OEM only & OEM must submit a report indicating compliance to reference architecture and best practices. The bidder to make necessary arrangement for the same and National Operation Center (NOC) will not pay any additional cost for implementation/configuration by OEM.

- All related documents, manuals, catalogues, and information furnished by the bidder shall become the property of the National Operation Center (NOC). Detailed process documentation, and SOP‟s (Standard Operating Procedure) should be submitted before project signoff.
- National Operation Center (NOC) may opt for Audit through a third party Authorized Agency or by the Terminal officials for the supplied hardware and Software. Successful bidder is required to coordinate with the Terminal Officials& Audit agency execute relevant test cases.
- National Operation Center (NOC) will have a periodic review of technology. Successful bidder will supply the models approved as per technical aspects. In case any of the models becomes end of support during entire contract period, then Successful bidder will provide the latest model available at no extra cost to National Operation Center (NOC) without disruption in performance of services/applications.
- During the Contract Period, in case there is hardware failure three or more times in a period of less than three (3) months, then it shall be replaced by equivalent or higher-level new equipment by the Successful bidder at no cost to the National Operation Center (NOC).
- The Bidder/OEM must Proposed a scalable, turnkey **VOIP solution** supporting over **100 concurrent calls** external, and inter-site communications.
- Five sites will be integrated with the National Operation Center (NOC) using a SIP trunk. The National Operation Center (NOC) will also be connected to Telecom Egypt for external call services.
- All quantities mentioned in this tender are subject to change based on the final design specifications.

2.2.2 DELIVERY ACCEPTANCE TEST

- All the delivered hardware items may be subjected to an acceptance test. Successful bidders must arrange one Engineer at the site at the date and time mentioned by the National Operation Center (NOC) to assist in the acceptance test.
- The successful bidder shall submit test report. The report should include the below contents:
    a. Test case
    b. Test case description
    c. Expected result
    d. Actual result
    e. Pass / fail
    f. Screen capture of the result

2.2.3 SUPPLY AND DEPLOYMENT

- The **VOIP solution** should be deployed in High availability Mode by OEM. All the components of **VOIP solution** such as VOIP OS, management software should be factory installed and shipped ready for fast deployment.
- The accessories of **VOIP solution** (including cables, rack mounting kit, Power strip in the rack etc.) required for the installation and configuration of the equipment will also be supplied by the successful Bidder.
- The Successful Bidder is responsible for all materials like SFP /Ethernet modules cables, connectors etc., equipment's, and services, specified or otherwise.
- Bidder shall be responsible for delivery and installation of the complete solution (hardware and software including compute and network resources) ordered at NOC requirement. Installation means mounting of **VOIP solution** in Rack (If any) and "Power-On" all the hardware with all the accessories provided with the hardware.
- Deployment of **VOIP solution** in the live network environment with high availability (HA) configuration in site.
- The Successful Bidder is responsible for all unpacking and shall carry out the installation, commissioning, and configuration of all the hardware & appliances and related software as required during the installation.
- The selected bidder should provide a full proof project execution plan before implementing the solution. The project execution plan should be without any network security breach.
- The project should roll out as per execution plan upon approval from the National Operation Center (NOC) IT management.
- The supply and installation of ordered items along with necessary setup, operational and user manuals / drawings, hardening guide, system test report, circuit diagram, if any etc., shall be made available and handed over to National Operation Center (NOC) after installation.
- The Bidder shall 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 be provisioned according to the requirements of the solution.
- The bidder shall provision for any components, subcomponents, assemblies, subassemblies as part of the **VOIP solution** in the bid response. In case the bidder has not provisioned for the above, the same shall be provisioned to meet solution requirements at no additional cost and time implications to the purchaser.
- The testing of all equipment & appliances and its operations shall be the responsibility of successful bidder and its OEM. They shall also accomplish all adjustments necessary for successful and continuous operation of these Hardware and software supplied, installed & commissioned under this tender.

2.2.4 CONFIGURATION AND COMMISSIONING

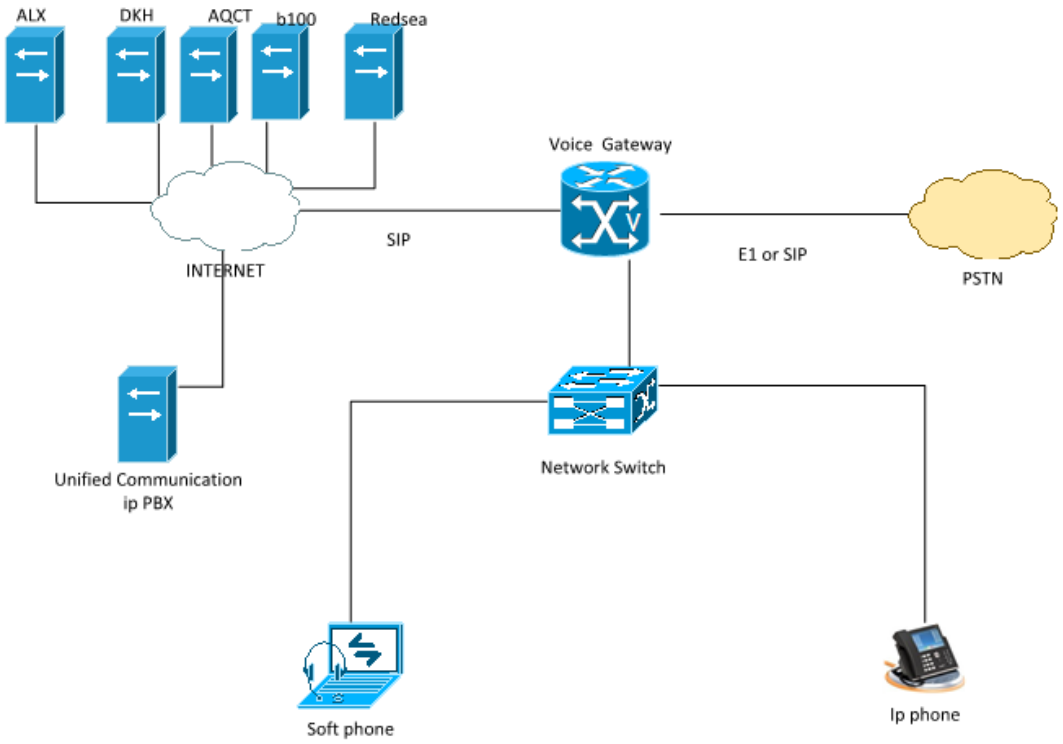
- The Successful Bidder shall be responsible for commissioning of the items supplied by preparing interfacing / integrating with purchaser's equipment / accessories / supplied by other vendors Integration and configuration of the **VOIP solution** as per the compliance sheet and international best practices.
- Configuration of **VOIP solution** management interfaces for unified management of all VOIP system resources.
- OEM will be responsible for Install and configure VOIP software, including all necessary licenses also Will responsible for Install and configure all VOIP hardware and Configuration of High Availability (HA).
- Acceptance Criteria of Commissioning

The following criteria must be met for acceptance of the VoIP solution:

1. Performance Testing:
   - Conduct tests demonstrating the ability to handle over 100 concurrent calls external and internal without degradation in quality.
2. Integration Success:
   - Successful integration with existing Cisco and Avaya systems for seamless communication.
3. Security Compliance:
   - Complete a security audit confirming compliance with CIS benchmarks.
4. User Acceptance Testing (UAT):
   - Complete user acceptance testing to confirm all functionalities meet operational needs.
5. Documentation and Training:
   - Hand over comprehensive documentation, including system architecture, user manuals, and training materials.
6. Acceptance testing:
   - must be completed within 30 days of system installation, with feedback and adjustments incorporated as needed.

2.3 Technical Specification / Requirement

2.3.1 TECHNICAL SPECIFICATION FOR VOIP SOLUTION



- **System Compatibility:**
  - The VoIP solution must seamlessly integrate with existing Cisco Call Manager and Avaya IP Office systems, ensuring efficient call routing and management.
- **High Availability and Backup:**
  - Ensure high availability with automatic failover mechanisms.
  - Implement automated backups for configuration settings, user data, and call logs at predefined intervals, stored securely for quick restoration.
- **Firmware and Software Upgrades:**
  - Perform necessary upgrades for video conference hubs to the latest recommended versions.
  - Upgrade firmware for all IP phones, Unified Communications IP PBX, and virtual machines to the latest recommended versions, including installation of the latest device pack.
- **Security Compliance:**
  - Adhere to CIS benchmarks for security.
  - Support AES encryption (minimum AES 256) for signaling and media.
  - Utilize TLS and SIP SRTP for secure communications.
- **Supported Protocols:**
  - SIP, H.323, RTP, SRTP, MGCP, H.264, and H.263 for video conferencing.
- **Call Control Features:**
  - Include point-to-point video solutions.
  - Provide a web-based interface for management.

    - Enable users to log into any phone to access their settings.
- **Quality of Service (QoS):**
    - Implement QoS mechanisms (e.g., 802.1p/q, RSVP) to optimize performance.

2.3.2 Integration Requirements

- **With Cisco Systems:**
    - Compatibility with Cisco Call Manager for seamless communication and call routing.
- **With Avaya Systems:**
    - Integration with Avaya IP Office for direct dialing and call transfers.
- **Interoperability:**
    - Facilitate inter-site calling and management to ensure effective communication between systems.

2.3.3 IP Phones and Softphone Specifications

- **IP Phones:**
    - Must feature an external speaker and a high-resolution, widescreen VGA backlit color display including their seats.
    - High-resolution LCD or touchscreen interface (minimum 5 inches) for easy navigation and call management.
    - Support high-definition audio (G.722) and standard codecs (G.711, G.729).
    - Full-duplex speakerphone with echo cancellation and noise reduction.
    - High-definition audio for crystal-clear sound quality.
    - Adjustable volume controls for both speaker and microphone.
    - Support for SIP and other relevant VoIP protocols.
    - Dual Ethernet ports (one for network connection and one for PC) with Power over Ethernet (PoE) support.
    - Call waiting and caller ID functionality.
    - Support for multiple lines (e.g., 2-6 lines) with call features like hold, transfer, and forwarding.
    - Include programmable keys,
    - Optional expansion modules for additional line keys or features.
    - Support for encryption protocols (SRTP, TLS) to ensure secure communications, and 802.1x authentication for security.
    - Optional AC power adapter.
    - Automatic registration with the Unified Communications IP PBX upon startup.
    - The IP phone model must be a current, state-of-the-art design that meets modern VoIP standards; legacy models will not be accepted.
    - User authentication options for secure access.
    - Capability to enter authorization codes for international calls without additional configuration.
- **Meeting Rooms IP Phones:**

    - Size: Minimum 5-inch display for easy navigation.
    - Features: Intuitive user interface for call management, calendar integration, and access to meeting tools.

- High-Quality Speaker: Full-duplex speakerphone with noise cancellation for clear audio during meetings.
- Microphone Array: Multiple microphones for 360-degree voice pickup to ensure all participants can be heard.
- Support for SIP and other relevant protocols for seamless integration with existing VoIP systems.
- Ethernet ports and Wi-Fi capability for flexible networking options.
- Optional support for video conferencing features, including a camera and video output.
- Compatibility with popular conferencing tools (e.g., Zoom, Microsoft Teams).
- Calendar integration for quick access to scheduled meetings.
- Automatic registration with the Unified Communications IP PBX upon startup
- Power over Ethernet (PoE) support for simplified installation.
- Optional AC power adapter.
- Ability to enter authorization codes for international calls without requiring additional accessories or installations.
- Programmable keys for quick access to frequently used functions.
- Support for multiple lines and call features (e.g., call hold, transfer, and forwarding).
- Encryption support for secure communications.
- User authentication options for secure access.

- **Softphones:**

  - Compatible with Windows, macOS, iOS, and Android.
  - Support HD voice/video, presence status, instant messaging, and conferencing.
  - Automatic registration with the Unified Communications IP PBX upon startup
  - Ability to create custom hotkeys for frequently used functions.
  - Configurable settings for call preferences, audio devices, and notifications.
  - User authentication options for secure access.
  - Compatibility with USB headsets and peripherals for enhanced audio experience.
  - Support for encryption protocols (e.g., SRTP, TLS) to ensure secure communication.
  - Capability to enter authorization codes for international calls without additional configuration.
  - Compatibility with major VoIP systems and protocols (SIP).
  - Real-time status updates (available, busy, away) to inform users of availability.
  - Supports features such as call hold, transfer, forwarding, and conferencing.

2.3.4 UNIFIED COMMUNICATIONS CLOUD IP PBX FEATURES

- Operate in a redundant structure to ensure uninterrupted call continuity.
- Intelligent call routing options including time-based, location-based, and skills-based routing.
- Call Forwarding Options for forwarding calls to different extensions or external numbers.
- Ability to transfer calls between users easily.
- Receive voicemail messages as audio files via email.

- Multi-party conference calling capabilities with easy setup.
- Licenses must cover all endpoints and users, including external and inter-site communications calls across sites.
- Support for secure communication protocols (TLS, SRTP).
- Robust authentication methods to ensure secure access.
- Support callback features and call parking, allowing retrieval of parked calls from any phone.
- Provide error alerts via voice and visual notifications.
- Easy-to-use interface for administrators to manage users and settings.
- Regular automated backups of system settings and user data.
- Ability to connect and manage multiple office locations seamlessly.
- Ability to add more users and features without significant hardware changes.
- A personal address book must be included, and the system must feature a web-based interface with all configurations stored in a database.
- Mechanisms to prioritize voice traffic to ensure high call quality, especially during peak usage.
- Advanced reporting features for call metrics, user activity, and system performance.
- Ability to integrate with other software solutions.
- Ability to set up customizable IVR menus for efficient call handling.

seat user's subscription for Unified Communications IP PBX softphones.	77
IP phone with external speaker and minimum 5-in. high-resolution (800 x 480) widescreen VGA backlit color display including their seats.	18
Operator IP phone	1
Meeting Rooms IP Phones	2

2.4 Security and Compliance

- The Bidder /OEM Should ensure necessary security features are built into the proposed VOIP solution.
- The Bidder /OEM is responsible for remediation of cybersecurity vulnerability on software and hardware with no additional cost to National Operation Center (NOC)
- The Bidder /OEM is responsible for Implementation of security measures and policies in alignment with ISO, PCI-DSS, and other relevant compliance standards.
- The Bidder /OEM is responsible for Configuration of integrated security features such as encryption, access controls, and advanced threat protection.
- The Bidder /OEM Should ensure necessary compliance and security hardening as per National Operation Center (NOC) policies/requirements and submitting recommendations for further improvements to mitigate any possible threats, effective compliance check, better visibility, and controls, etc.

2.5 Training and Documentation

- The Bidder /OEM Should Ensuring a smooth handover with detailed documentation and training provided to the National Operation Center (NOC) IT team.
- Installation and Configuration Documentation (documentation shall include screenshots for steps performed). Standard Operating Procedures (SOP) to be provided for startup-shutdown of **VOIP solution**, add, or remove IP Phones, trunk, call routing from VOIP.
- The bidder/OEM shall provide a detailed drawing of the installed setup after completion of the project. This will also include the printout of important configuration settings of the solution.
- The OEM should provide a detailed architecture of the provided solution along Installation and Administration guide which must include High-level Design (HLD) and Low-Level Design (LLD).
- VOIP solution diagram.
- detailed BOQ for proposed VOIP solution.
- separate sheet for specification/white paper of the products.

2.6 Project Reporting and Handover

- Submission of commissioning reports detailing the deployment and configuration of the **VOIP solution**.
- Provision of a comprehensive project completion report summarizing all activities, configurations, and outcomes.

2.7 Maintainability and Warranty Support

The scope under warranty shall cover to provide services as described below:

All delivered items Hardware and System software in this tender should be monitored and serviced in such a manner to ensure maximum uptime and performance levels. The guarantee/warranty should be of the highest nature extended by the OEM on the date of participation in the Tender (Necessary documentary evidence to be submitted).

2.7.1 Maintainability

- The Bidder will have to submit an undertaking from OEM assuring the availability of requisite spare parts for hardware (if any) the maintainability period of 5 (five) years from the date of installation.
- The software & hardware quoted by the bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 5 years of the Purchase order/contract period. In the event of the supplied equipment being declared End of Support/End of Life during

the contract period of 5 (five) years, the bidder must replace the equipment with equipment having an equivalent or higher model.

2.7.2 WARRANTY SUPPORT

- Original Equipment Manufacturer (OEM) should have online 24 x 7 support for any hardware or software-related issue. The proposed solution should have one window support solution for all the components including hardware, firmware, and software used. The support should be from OEM.

- **VOIP solution** must have direct OEM, L1, L2, and L3 support, 24x7x365 days with unlimited incident support (Telephonic / Web / Email) and technical contacts/contract within 4-hour response time including unlimited upgrades and updates during the tender specific warranty period.

- Provide on-site comprehensive warranty for the supplied items - equipment/system/subsystems (hardware and system software) for a period of 3 (three) years with 24x7 x 365 remote support and maximum resolution of NBD. The hardware equipment (if any) should be guaranteed/warranted against all defects and failure and such guarantee/warranty shall include replacement of defective parts/equipment and/or repair of the same free of cost. All warranty shall be onsite. The bidder should confirm in their response that the support during the warranty period would be carried out by the OEM for the respective equipment / peripheral. The bidder should also ensure that the SLA (24 x 7 x 365 support with a maximum resolution time of NBD) is adhered to, and this must be articulated in the bid response as well. The warranty shall also cover the following:

    a) Installation / re-installation / maintenance / reconfiguration of System software and other supplied software

    b) All system patches, upgrades, service packs, etc. of the OS and all other software supplied must be made available free of charge.

    c) Support for integration and update of infrastructure/network configuration and change management of the entire solution (existing as well as that procured as the scope of this tender) to meet business requirements.

    d) Any change in the IP scheme, if required, limited to all the equipment installed at the Data Centre should be done in consultation with the NOC IT team.

- The non-delivery of services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP.

- In case of item replacement with a new one, the new item must be at least the same model, and in case the replacement is a higher model must be compatible with the NOC. environment and technically approved by NOC

2.8 UPGRADES AND UPDATES

- The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Appliance/hardware & software provided free of charge during the contract period. If, however, the upgrades/updates are not available then the support for the implemented Solution/ Appliance/hardware & software should be available at any point of time. The solution (software or hardware or both) provided by the successful bidder should not be declared end of sale within 3 years of sign-off of the project. If at all the solution (software or hardware or both) is declared end of sale within 3 years of sign-off, the successful bidder must provide the upgraded version (software or hardware or both) free of charge, to the NOC.
- The solution should provide seamless upgrades for (but not limited to) Firmware, software, BIOS, and other such functions which are required in the solution. All patches for the complete hardware and software solution must come from a single validated source. It should be possible to apply and upgrade all software and hardware-related firmware and patches from the same GUI that is used to manage the **VOIP solution**.

2.9 Additional Consideration

Payment terms per project - 25% advance payment against non-conditional LG , 25% against delivery of Items, 40% after final commissioning & signoff -10% retention until end of the warranty period.

2.10 Levels of Service

The Supplier's goal must be to meet, and even exceed, when possible, the levels of service described.

3 CCTV AND ACCESS CONTROL PROJECT

3.1 PURPOSE OF THE PROJECT:

The purpose of this RFP is to invite technically and commercially competitive proposals from reputed manufacturers/authorized representatives for **CCTV and Access Control solution.** The vendor engagement will involve Supply, Installing, Configuring, Testing, Implementing, and Commissioning of the new solution, as well as providing incident and product support as per Scope of work and Technical Specifications given in this RFP, at National Operation Center (NOC) Datacenter.

3.2 SCOPE of work

- The broad scope of work as detailed in this section refers to the Hardware and System software that is procured through this tender and used for Supply, Installing, Configuring, Testing, Implementing and Commissioning of **CCTV and Access Control solution** the at National Operation Center (NOC).

- **Licensing Coverage**: The bidder/OEM must ensure that all necessary licenses for the **CCTV and Access Control solution** are fully covered
- **Responsibility for Additional Licenses**: If any licenses needed to complete the solution are identified after the proposal is submitted, the bidder/OEM will be responsible for covering the costs of those additional licenses.
- **this scope of work shall include, but not be limited to, the following:**

3.2.1 GENERAL CONDITIONS

- **CCTV and Access Control solution should have same Management system**

- The OEM shall be responsible for Design, Supply, Installation, Configuration, Testing and Commissioning of the **CCTV and Access Control solution** in at National Operation Center (NOC).

- The OEM shall be doing the Project Management for the entire Project from commencement to final handing over for live use. The proposed solution must be supported for a period of 3 years as per RFP and National Operation Center (NOC) requirement.

- The OEM must prepare architecture design, optimize network to increase performance, documentation, and project plan as part of the implementation services.

- Installation and configuration of supplied hardware associated system software and system integration must be carried out by Bidder.

- The bidder must submit a detailed plan for implementation of the solution. The plan should include the full scope of the project as mentioned above. On acceptance of such plan by National Operation Center (NOC), the OEM is required to carry out the implementation, customization as applicable including supply, installation, and testing of solution etc. The OEM shall also handle all matters relating to the configuration and operation of the system including but not limited to application, system interfaces, documentation, user manual and training for the successful implementation of the system. The project plan update to be published bi-weekly till the project completion.

- The Bidder/OEM shall be responsible for performing the necessary changes in the configuration required for Hardening and/or request directed by security team & audit team.

- The Bidder/OEM shall be responsible for firmware patches/bug, fixes BIOS upgrade and Version Upgrade of software.

- The Bidder/OEM shall be responsible for generation and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams and other reports etc. All such documents shall commence only after the same is approved by National Operation Center (NOC).
- The Bidder/OEM should provide a detailed project plan in terms of activity and phase-wise timelines (no. of days) required for executing the project with the details of deliverables and milestones including the delivery of Server components. The Bidder/OEM shall inform the name of the Project Manager who would be the single point of contact during the complete project implementation.
- The Bidder/OEM shall be responsible for installing / configuring of all patches / updates / upgrades required for the offered solution without any extra cost to National Operation Center (NOC) during the warranty period.
- All service requests for **CCTV and Access Control solution** should be received, managed, executed, and tracked to closure by the OEM or through Authorized Service Provider.
- The bidder shall Plan & Design the Architecture services from the OEM. The entire hardware and software supplied under this RFP must be installed and configured by OEM only & OEM must submit a report indicating compliance to reference architecture and best practices. The bidder to make necessary arrangement for the same and National Operation Center (NOC) will not pay any additional cost for implementation/configuration by OEM.
- All related documents, manuals, catalogues, and information furnished by the bidder shall become the property of the National Operation Center (NOC). Detailed process documentation, and SOP‟s (Standard Operating Procedure) should be submitted before project signoff.
- National Operation Center (NOC) may opt for Audit through a third party Authorized Agency or by the Terminal officials for the supplied hardware and Software. Successful bidder is required to coordinate with the Terminal Officials& Audit agency execute relevant test cases.
- National Operation Center (NOC) will have a periodic review of technology. Successful bidder will supply the models approved as per technical aspects. In case any of the models becomes end of support during entire contract period, then Successful bidder will provide the latest model available at no extra cost to National Operation Center (NOC) without disruption in performance of services/applications.
- During the Contract Period, in case there is hardware failure three or more times in a period of less than three (3) months, then it shall be replaced by equivalent or higher-level new equipment by the Successful bidder at no cost to the National Operation Center (NOC).
- The Bidder/OEM must Proposed a scalable, turnkey **CCTV and Access Control solution**

- All quantities mentioned in this tender are subject to change based on the final design specifications.

3.2.2 DELIVERY ACCEPTANCE TEST

- All the delivered hardware items may be subjected to an acceptance test. Successful bidders must arrange one Engineer at the site at the date and time mentioned by the National Operation Center (NOC) to assist in the acceptance test.
- The successful bidder shall submit test report. The report should include the below contents:
    a. Test case
    b. Test case description
    c. Expected result
    d. Actual result
    e. Pass / fail
    f. Screen capture of the result

3.2.3 SUPPLY AND DEPLOYMENT

- The accessories of **CCTV and Access Control solution** required for the installation and configuration of the equipment will also be supplied by the successful Bidder.
- Bidder shall be responsible for delivery and installation of the complete solution (hardware and software) ordered at National Operation Center (NOC) requirement.
- The Successful Bidder is responsible for all unpacking and shall carry out the installation, commissioning, and configuration of all the hardware & appliances and related software as required during the installation.
- The selected bidder should provide a full proof project execution plan before implementing the solution. The project execution plan should be without any network security breach.
- The project should roll out as per execution plan upon approval from the National Operation Center (NOC) IT management.
- The supply and installation of ordered items along with necessary setup, operational and user manuals / drawings, hardening guide, system test report, circuit diagram, if any etc., shall be made available and handed over to National Operation Center (NOC) after installation.
- The Bidder shall 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 be provisioned according to the requirements of the solution.

- The bidder shall provision for any components, subcomponents, assemblies, subassemblies as part of the **CCTV and Access Control solution** in the bid response. In case the bidder has not provisioned for the above, the same shall be provisioned to meet solution requirements at no additional cost and time implications to the purchaser.
- The testing of all equipment & appliances and its operations shall be the responsibility of successful bidder and its OEM. They shall also accomplish all adjustments necessary for successful and continuous operation of these Hardware and software supplied, installed & commissioned under this tender.

3.2.4 CONFIGURATION AND COMMISSIONING

- The Successful Bidder shall be responsible for commissioning of the items supplied by preparing interfacing / integrating with purchaser's equipment / accessories / supplied by other vendors Integration and configuration of the **CCTV and Access Control solution** as per the compliance sheet and international best practices.
- Configuration of **CCTV and Access Control solution** management interfaces for unified management of all **CCTV and Access Control** system resources.
- Video stream recording will be 25 days for all camera along the day with 15 FPS with resolution FHD.
- Install, Configure, Startup the mentioned System with all components and ensure compatibility and operation stability.
- OEM will be responsible for Install and configure **CCTV and Access Control** software, including all necessary licenses.
- Acceptance Criteria of Commissioning

The following criteria must be met for acceptance of the **CCTV and Access Control** solution:

1. Acceptance Criteria for Commissioning of CCTV Systems

   - ✓ **System Functionality**: Ensure all cameras are operational and provide clear, high-quality images.
   - ✓ **Coverage Verification**: Confirm that all designated areas are covered as per the project specifications.
   - ✓ **Network Integration:** Verify that all cameras are properly integrated into the network and can be accessed remotely.
   - ✓ **Recording and Storage:** Check that the recording system is functioning correctly, and that storage meets the required capacity and retention policies.
   - ✓ **Alarm and Notification:** Ensure that all alarm and notification systems are working and correctly configured.

- ✓ **User Training:** Provide comprehensive training to the end-users on system operation and maintenance.
- ✓ **Documentation:** Complete and hand over all necessary documentation, including system manuals, configuration settings, and maintenance schedules.

2. Acceptance Criteria for Commissioning of Access Control Systems

- ✓ **System Functionality:** Verify that all access control points (e.g., doors, gates) are operational and respond correctly to authorized and unauthorized access attempts.
- ✓ **Integration with Other Systems:** Ensure seamless integration with other security systems, such as CCTV and alarm systems.
- ✓ **User Authentication:** Test all authentication methods (e.g., keycards, biometrics) to ensure they function correctly.
- ✓ **Access Logs:** Confirm that access logs are being accurately recorded and stored as per the project requirements.
- ✓ **Emergency Protocols:** Verify that emergency access protocols (e.g., fire alarm integration, emergency exits) are correctly implemented and functional.
- ✓ **User Training:** Provide training to the end-users on how to operate and manage the access control system.
- ✓ **Documentation:** Ensure all relevant documentation, including user manuals, system configurations, and maintenance procedures, is complete and handed over to the client.

3.3 Technical Specification / Requirement

3.3.1 Indoor Fixed Cameras – QTY (10)

1- Image sensor: 1/2.8" progressive scan CMOS
2- High Quality Lens with wide Horizontal field of view (over 90°)
3- Camera angle adjustment for Pan, tilt and rotation
4- Support Light finder 2.0, Wide dynamic range, Day and Night functionality, multi-view streaming, Autofocus, IP rating.
5- Work under any light conditions.
6- Include Local storage (memory card included with Min. 64GB)
7- Operating temperature Range: 0 to 50 °C
8- Resolution: 1920x1080（2MP）
9- Video streaming: Multiple, individually configurable streams in H.264, H.265 and Motion JPEG with Controllable frame rate and bandwidth
10- Pan/Tilt/Zoom: Digital PTZ
11- Compression: Support Zipstream, H.264, H.265, Motion JPEG

12- Network: RJ45 10BASE-T/100BASE-TX PoE
13- Security features must include Signed firmware, Secure boot, https, tls1.2, IP Address Filtering, network access control, user access log.
14- PoE midspan and Mount suit suitable for wall must be included.
15- Warranty 3 years for camera and all accessories.

3.3.2 CCTV VMS SOFTWARE

1- Base VMS Perpetual License
2- Unrestricted number of IP camera per recording server
3- Unrestricted numbers of users
4- Centralized management, Alarm Manager and Flexible event rule engine
5- Support installation of client on windows OS, Open camera view through Web Client and Mobile application
6- Microsoft Active Directory integration and Kerberos authentication, MFA is preferred.
7- Support H.264, H.265, MJPEG, MPEG-4, MPEG-4 ASP & MPEG, Metadata, Hardware accelerated video decoding.
8- Media database encryption and digital signing
9- Camera, Management and Recording Server communication encryption with tls1.2
10- Build more than one camera view and assign each one to certain group of user operator.
11- Restrict client feature based on the user rule.
12- Restrict Live view and playback in VMS client on workstation security operator based on user rule.
13- Must be compatible with delivered camera model.
14- The software will be installed on VMS server in IT Datacenter.
15- VMS software must be compatible with VMS server and storage (End to End Solution).
16- Support License with warranty 3 years 8 hours/5 days support.

3.3.3 CCTV VMS SERVER AND STORAGE

Require solution and specs (Processor 2 socket, RAM, Network Bandwidth, etc.) for server and storage capacity to cover the following:

1- Number of cameras with 15 FPS with full resolution between the server and camera and between the server and a lot of operator computer.
2- Video stream recording will be 25 days for all camera along the day (24 Hours) with 15 FPS with full resolution.
3- Server and storage items must be redundant in their component as but not limited to Processor, RAM, Network Port, Power Supply, Disk Storage with disk array for operating system and live and recording video stream disk with proper disk array.
4- VMS server and internal storage must be compatible with VMS software (End To End Solution).
5- Warranty 3 Years for server and storage.

3.3.4 THE ACCESS CONTROL SOFTWARE

1- Should be the same VMS management software
2- The application should have a friendly interface and ease of management with good built-in help in the software application.
3- The Application must contain a built-in powerful Monitoring system to manage hardware devices (EX: Controller, Door, etc.) and alert by email in case an event has occurred and to keep the events in the database for more analysis in the feature.
4- The application must contain built-in powerful reporting tools about the events that happened on the controlled door.
5- Employees should be uniquely identified using the current staff ID.
6- Ability to change the controlled door status (Locked, Unlocked) from the application.
7- Multiple security levels with the ability to create custom levels based on the requested permissions to manage the software.
8- Security audit according to any modifications in the application.
9- Ability to open more than one concurrent connection from different operators at the same time to manage the application.
10- Ability to backup and restore (automatic schedule or manual).
11- Ability to integrate with other systems for creating employees (users), printing the cards, and disabling employees.
12- The system shall have the ability to immediately send invalid access transactions via email with necessary information.
13- Invalid access status shall include an expired badge, lost badge, retired badge or suspended badge.
14- The application should keep track of the number of printed cards per employee.
15- The system database shall be protected from unauthorized access or inadvertent modification.
16- The system should have the ability to set time zones.
17- Delivered license must meet our access cards and controlled doors.
18- Must include integration between AC system and Fire Alarm system to open all doors in case fire alarm activated.

3.3.5 STANDALONE ACCESS CONTROLLER – QTY (2)

1- Full compatibility with software application and reader's hardware.
2- Controller must include the card reader as standalone device and must include the necessary wired terminals to connect it with other access control components like exist button and Electric Door Strike lock with build in door contact.
3- Include network interface to communicate with access control system.
4- Keep access permissions in case of restart.
5- Possibility to start and work properly with the reader in case the application is not available, or the controller starts before the software application.
6- Machine must accept the employee transaction and store the transaction locally in case the access control application is offline and when the application become online the transaction have been pulled automatically from the machines without data loss.

7- Access control machine must have the ability to authenticate employee against biometric finger and card ID.
8- Machine must have High capacity with min. 1,000 card IDs in authorized user list, and 100,000 logs.
9- in case of finger biometric detection method is used in access control, the machine must have fake finger detection, duress finger, timed anti-pass back.
10- Machine must be certified with IP65 rated, IP66 preferred.
11- Machine must have ethernet port for network connection and communication with access control software.
12- Access control machine must have the ability to be enroll station to enroll employee access card and biometric finger in his profile in access control software.

The access control system must also provide, additional components:

1- Electric Door Strike lock (Holding Force: 1200lbs) with build in door contact.
2- Standalone access control device biometric finger with Card Readers (**Mifare**).
3- Card (QTY: 500) to be compatible with card reader.
4- Card Printer with support to print card on **both side** with any license required and related software printer driver and card design.
5- Card printer ribbons to cover printing 500 card on **both sides**.
6- 2 clean kit for printer
7- Contactless Exit Button.
8- Deliver and install complete cabling system between all access control component.

3.4 Security and Compliance

- The Bidder /OEM Should ensure necessary security features are built into the proposed **CCTV and Access Control solution**.
- The Bidder /OEM is responsible for remediation of cybersecurity vulnerability on software and hardware with no additional cost to National Operation Center (NOC)
- The Bidder /OEM is responsible for Implementation of security measures and policies in alignment with ISO, PCI-DSS, and other relevant compliance standards.
- The Bidder /OEM is responsible for Configuration of integrated security features such as encryption, access controls, and advanced threat protection.
- The Bidder /OEM Should ensure necessary compliance and security hardening as per National Operation Center (NOC) policies/requirements and submitting recommendations for further improvements to mitigate any possible threats, effective compliance check, better visibility, and controls, etc.

3.5 Training and Documentation

- The Bidder /OEM Should Ensuring a smooth handover with detailed documentation and training provided to the National Operation Center (NOC) IT team.

- Installation and Configuration Documentation (documentation shall include screenshots for steps performed). Standard Operating Procedures (SOP) to be provided for startup-shutdown of **CCTV and Access Control solution**.
- The bidder/OEM shall provide a detailed drawing of the installed setup after completion of the project. This will also include the printout of important configuration settings of the solution.
- The OEM should provide a detailed architecture of the provided solution along Installation and Administration guide which must include High-level Design (HLD) and Low-Level Design (LLD).
- **CCTV and Access Control solution** diagram.
- detailed BOQ for proposed **CCTV and Access Control solution**.
- separate sheet for specification/white paper of the products.

3.6 Project Reporting and Handover

- Submission of commissioning reports detailing the deployment and configuration of the **CCTV and Access Control solution**.
- Provision of a comprehensive project completion report summarizing all activities, configurations, and outcomes.

3.7 Maintainability and Warranty Support

The scope under warranty shall cover to provide services as described below:

All delivered items Hardware and System software in this tender should be monitored and serviced in such a manner to ensure maximum uptime and performance levels. The guarantee/warranty should be of the highest nature extended by the OEM on the date of participation in the Tender (Necessary documentary evidence to be submitted).

3.7.1 Maintainability

- The Bidder will have to submit an undertaking from OEM assuring the availability of requisite spare parts for hardware (if any) the maintainability period of 5 (five) years from the date of installation.
- The software & hardware quoted by the bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 5 years of the Purchase order/contract period. In the event of the supplied equipment being declared End of Support/End of Life during the contract period of 5 (five) years, the bidder must replace the equipment with equipment having an equivalent or higher model.

3.7.2 WARRANTY SUPPORT

- Original Equipment Manufacturer (OEM) should have online 24 x 7 support for any hardware or software-related issue. The proposed solution should have one window support solution for all the components including hardware, firmware, and software used. The support should be from OEM.

- **CCTV and Access Control solution** must have direct OEM, L1, L2, and L3 support, 24x7x365 days with unlimited incident support (Telephonic / Web / Email) and technical contacts/contract within 4-hour response time including unlimited upgrades and updates during the tender specific warranty period.

- Provide on-site comprehensive warranty for the supplied items - equipment/system/subsystems (hardware and system software) for a period of 3 (three) years with 24x7 x 365 remote support and maximum resolution of NBD. The hardware equipment (if any) should be guaranteed/warranted against all defects and failure and such guarantee/warranty shall include replacement of defective parts/equipment and/or repair of the same free of cost. All warranty shall be onsite. The bidder should confirm in their response that the support during the warranty period would be carried out by the OEM for the respective equipment / peripheral. The bidder should also ensure that the SLA (24 x 7 x 365 support with a maximum resolution time of NBD) is adhered to, and this must be articulated in the bid response as well. The warranty shall also cover the following:

    e) Installation / re-installation / maintenance / reconfiguration of System software and other supplied software

    f) All system patches, upgrades, service packs, etc. of the OS and all other software supplied must be made available free of charge.

    g) Support for integration and update of infrastructure/network configuration and change management of the entire solution (existing as well as that procured as the scope of this tender) to meet business requirements.

    h) Any change in the IP scheme, if required, limited to all the equipment installed at the Data Centre should be done in consultation with the NOC IT team.

- The non-delivery of services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP.

- In case of item replacement with a new one, the new item must be at least the same model, and in case the replacement is a higher model must be compatible with the NOC. environment and technically approved by NOC

3.8 UPGRADES AND UPDATES

- The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Appliance/hardware & software provided free of charge during the contract period. If, however, the upgrades/updates are not available then the support for the implemented Solution/ Appliance/hardware & software should be available at any point of time. The solution (software or hardware or both) provided by the successful bidder should not be declared end of sale within 3 years of sign-off of the project. If at all the solution (software or hardware or both) is declared end of sale within 3 years of sign-off, the successful bidder must provide the upgraded version (software or hardware or both) free of charge, to the NOC.
- The solution should provide seamless upgrades for (but not limited to) Firmware, software, BIOS, and other such functions which are required in the solution. All patches for the complete hardware and software solution must come from a single validated source. It should be possible to apply and upgrade all software and hardware-related firmware and patches from the same GUI that is used to manage the **CCTV and Access Control solution**.

3.9 Additional Consideration

Payment terms per project - 25% advance payment against non-conditional LG, 25% against delivery of Items, 40% after final commissioning & signoff -10% retention until end of the warranty period.

3.10 Levels of Service

The Supplier's goal must be to meet, and even exceed, when possible, the levels of service described.

4 INTERNET FIREWALL SOLUTION

4.1 PURPOSE OF THE PROJECT:

The purpose of this RFP is to invite technically and commercially competitive proposals from reputed manufacturers/authorized representatives for **Internet Firewall solution**. The vendor engagement will involve Supply, Installing, Configuring, Testing, Implementing, and Commissioning of the new solution, as well as providing incident and product support as per Scope of work and Technical Specifications given in this RFP, at National Operation Center (NOC) Datacenter.

4.2 SCOPE of work

- The broad scope of work as detailed in this section refers to the Hardware and System software for internet firewall that is procured through this tender and used for Supply, Installing, Configuring, Testing, Implementing, and Commissioning of the **Two (2) Internet Firewall** at National Operation Center (NOC).

- **Licensing Coverage**: The bidder/OEM must ensure that all necessary licenses for the **Internet Firewall solution** are fully covered.
- **Responsibility for Additional Licenses**: If any licenses needed to complete the solution are identified after the proposal is submitted, the bidder/OEM will be responsible for covering the costs of those additional licenses.

- **this scope of work shall include, but not be limited to, the following:**

4.2.1 GENERAL CONDITIONS

- Professional Services are requested for complete & full implementation and configuration for firewalls in National Operation Center (NOC).

- The OEM/bidder shall be responsible for Design, Supply, Installation, Configuration, Testing and Commissioning of the **Internet Firewall solution** in at National Operation Center (NOC).
- The OEM shall be doing the Project Management for the entire Project from commencement to final handing over for live use. The proposed solution must be supported for a period of 3 years as per RFP and National Operation Center (NOC) requirement.
- The OEM must prepare architecture design, optimize network to increase performance, documentation, project plan and training as part of the implementation services.
- Installation and configuration of supplied hardware associated system software and system integration must be carried out by OEM or authorize partner.
- Bidder/OEM should propose highly scalable solution. Solutions with limited scalability would not be acceptable to National Operation Center (NOC). Solutions which are not mature for over 1 year should not be quoted.
- The solution implemented should have high availability features to ensure that Network security will be available at any time of the day.
- The Bidder/OEM shall be responsible for performing the necessary changes in the configuration required for Hardening and/or request directed by security team & audit team.
- The Bidder/OEM shall be responsible for firmware patches/bug, fixes BIOS upgrade and Version Upgrade of software.
- The Bidder/OEM shall be responsible for generation and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams and other reports etc. All such documents shall commence only after the same is approved by National Operation Center (NOC).
- The Bidder/OEM should provide a detailed project plan in terms of activity and phase-wise timelines (no. of days) required for executing the project with the details of deliverables and milestones including the delivery of Server components. The Bidder/OEM shall inform the name of the Project Manager who would be the single point of contact during the complete project implementation.
- The OEM must analyze, review, and gather performance metrics and ensure it performs optimally.
- The Bidder/OEM shall be responsible for installing / configuring of all patches / updates / upgrades required for the offered solution without any extra cost to National Operation Center (NOC) during the warranty period.
- All service requests for **Internet Firewall solution** should be received, managed, executed, and tracked to closure by the OEM or through Authorized Service Provider.

- All related documents, manuals, catalogues, and information furnished by the bidder shall become the property of the National Operation Center (NOC). Detailed process documentation, and SOP‟s (Standard Operating Procedure) should be submitted before project signoff.

- National Operation Center (NOC) may opt for Audit through a third party Authorized Agency or by the Terminal officials for the supplied hardware and Software. Successful bidder is required to coordinate with the Terminal Officials& Audit agency execute relevant test cases.

- National Operation Center (NOC) will have a periodic review of technology. Successful bidder will supply the models approved as per technical aspects. In case any of the models becomes end of support during entire contract period, then Successful bidder will provide the latest model available at no extra cost to National Operation Center (NOC) without disruption in performance of services/applications.

- During the Contract Period, in case there is hardware failure three or more times in a period of less than three (3) months, then it shall be replaced by equivalent or higher-level new equipment by the Successful bidder at no cost to the National Operation Center (NOC).

- The Bidder/OEM must Proposed a scalable, turnkey **Internet Firewall solution**

4.2.2 DELIVERY ACCEPTANCE TEST

- All the delivered hardware items may be subjected to an acceptance test. Successful bidders must arrange one Engineer at the site at the date and time mentioned by the National Operation Center (NOC) to assist in the acceptance test.
- The successful bidder shall submit test report. The report should include the below contents:
    a. Test case
    b. Test case description
    c. Expected result
    d. Actual result
    e. Pass / fail
    f. Screen capture of the result

4.2.3 SUPPLY AND DEPLOYMENT

- The **Internet Firewall solution** should be deployed in High availability Mode by OEM. All the components of **an Internet Firewall solution** should be factory installed and shipped ready for fast deployment.

- The accessories of **Internet Firewall solution** (including cables, rack mounting kit, Power strip in the rack etc.) required for the installation and configuration of the equipment will also be supplied by the successful Bidder.

- The Successful Bidder is responsible for all materials like SFP /Ethernet modules cables, connectors etc., equipment's, and services, specified or otherwise.
- The bidder shall be responsible for delivery and installation of internet firewall ordered National Operation Center (NOC) requirement. Installation means mounting of **Internet Firewall solution** in Rack (If any) and "Power-On" all the hardware with all the accessories provided with the hardware.
- Deployment of **Internet Firewall solution** in the live network environment with high availability (HA) configuration in Data Center.
- The Successful Bidder is responsible for all unpacking and shall carry out the installation, commissioning, and configuration of all the hardware & appliances and related software as required during the installation.
- The selected bidder should provide a full proof project execution plan before implementing the solution. The project execution plan should be without any network security breach.
- The project should roll out as per execution plan upon approval from the National Operation Center (NOC) IT management.
- The supply and installation of ordered items along with necessary setup, operational and user manuals / drawings, hardening guide, system test report, circuit diagram, if any etc., shall be made available and handed over to National Operation Center (NOC) Unit after installation.
- The Bidder shall 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 be provisioned according to the requirements of the solution.
- The bidder shall provision for any components, subcomponents, assemblies, subassemblies as part of the **Internet Firewall solution** in the bid response. In case the bidder has not provisioned for the above, the same shall be provisioned to meet solution requirements at no additional cost and time implications to the purchaser.
- The testing of all equipment & appliances and its operations shall be the responsibility of successful bidder and its OEM. They shall also accomplish all adjustments necessary for successful and continuous operation of these Hardware's and software's supplied, installed & commissioned under this tender.

4.2.4 CONFIGURATION AND COMMISSIONING

- The Successful Bidder shall be responsible for commissioning of the items supplied by preparing interfacing / integrating with purchaser's equipment / accessories / supplied by other vendors Integration and configuration of the **Internet Firewall solution** as per the compliance sheet and international best practices.

- OEM/bidder will be responsible for Install and configure **Internet Firewall solution**, including all necessary licenses also Will responsible for Install and configure all **Internet Firewall solution** hardware and Configuration of High Availability (HA).
- OEM/bidder will be responsible for Integration between **Internet Firewall solution** and Core Network solution also Will be responsible for handling and solving any issue related to this integration with Core network vendor.
- **Acceptance Criteria of Commissioning**

The following criteria must be met for acceptance of the **Internet Firewall solution**:

1. **Technical Specifications**
    - The firewall must meet the specified technical requirements outlined in the tender, including:
        - Throughput capacity (e.g., minimum XX Gbps).
        - Concurrent connections (e.g., minimum XX million).
2. **Performance Testing**
    - Successful completion of performance tests demonstrating:
        - Latency measurements under load.
        - Scalability tests with varying traffic volumes.
3. **Security Features**
    - All features must be fully operational and configurable, such as:
        - Deep Packet Inspection (DPI).
        - Web filtering.
        - Application filtering.
        - Intrusion Detection and Prevention Systems (IDPS).
        - Virtual Private Network (VPN) support.
        - Threat intelligence and reporting capabilities.
        - SSL/TLS inspection.
        - Anti-malware and anti-bot protection.
        - Network Address Translation (NAT) and application proxy support.
4. **Deployment and Integration**
    - Installation procedures and integration with existing network infrastructure must be clearly defined, along with migration strategies if applicable.
5. **High Availability Testing**
    - The firewall must support high availability configurations, and successful testing of these configurations must be conducted to ensure:
        - Seamless failover between active and standby units without dropping sessions.
        - No disruption to users, with all sessions remaining active and intact during the failover process.
        - Verification that all features operate correctly when the failover is engaged, and that functionality returns to normal when the main unit is restored.
6. **Acceptance Testing**
    - Successful completion of acceptance testing within specified timelines, demonstrating that the firewall meets all agreed-upon specifications.
7. As the key deliverable, the firewalls must be online, fully tested, functional, and in a production environment for the project to be considered complete.

8. Implementation of management software for all firewalls devices is also required as part of project deliverables.
9. Run compliance and vulnerabilities scans on all hardware and software with the latest CIS benchmark.
10. Remediate any compliance or vulnerabilities findings.
11. The firewalls can support multiple route domains
12. System hardening for firewalls

4.3 Technical Specification / Requirement

4.2.1 GENERAL REQUIREMENTS:

- The solution must have 2 (two) hardware appliances that work as active/ passive solution, and they have a real time synchronization of any configuration change and with purpose-built OS.
- All devices must be delivered with two redundant power supplies.
- Must be high performance ASIC based appliance with multiple processing modules to provide Hardware Acceleration & minimal latency
- Must include all listed features from day one with no hidden costs
- Must be ICSA Labs certified for Enterprise Firewall and/or EAL 4 certified
- Must participate in NSS Labs NGFW, DCIPS & BDS reports, must be in Recommended zone.
- Must be leader in Latest Gartner Enterprise Firewall report.

4.3.2 PERFORMANCE REQUIREMENTS:

- IPv4/IPv6 Firewall throughput up to 70 Gbps.
- Firewall concurrent sessions up to 8M Sessions
- Firewall new sessions per second must be up to 550,000 sessions per second
- IPS throughput at least 14 Gbps with Enterprise Mix traffic.
- NGFW throughput at least 11.5 Gbps with Enterprise Mix traffic.
- Threat Protection throughput at least 10.5 Gbps with Enterprise Mix traffic.
- SSL Inspection throughput at least 9 Gbps

4.3.3 HARDWARE REQUIREMENTS

- Support at least 4 ports 25 Gigabit-Ethernet SFP+.
- Support at least 4 ports 10 Gigabit-Ethernet SFP+.
- Support at least 8 ports 1 Gigabit-Ethernet SFP.
- Support at least 16 ports 1 Gigabit-Ethernet RJ45.
- Support 2 integrated management ports.
- Support local Storage with at least 2x240 GB SSD.

4.3.4 MANAGEMENT & ADMINISTRATION

- Must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management within the same platform
- Must Support Administrator Password Policy
- Must support pre-defined view for operations center.

- May support configurable option to define remote access to the Firewall on any interface and restrict the same to a specific IP/Subnet (i.e., Trusted Hosts for Management)
- May support connecting directly to the firewall through a console connection (RJ45 or DB9)
- Must support SNMPv2c and SNMPv3
- Must support provisioning to generate automatic notification of events via mails / syslog
- Must support role-based administration of firewall
- Must support simultaneous login of Multiple Administrators.
- Must support exporting the firewall rules set and configuration to a text file via Web or TFTP
- Must Support Firmware Image upgrade via FTP, TFTP and WebUI
- Must support system software rollback to the previous version after upgrade

4.3.5 FIREWALL FEATURES:

- Must support Mixed Mode of operation (Routed & Bridged) on the same platform using virtual firewalls.
- Must support Configurable virtual systems resource limiting and management such as maximum/guaranteed 'active sessions and log disk quota
- Must support granular access control based on user or user group, traffic type, target or source IP address, interface or domain name, time of the day or day of the week.
- Firewall Policies must support profile-based mode & application-based mode.
- Must support Host Protection Engine to protect against DoS attacks
- Must support GeoIP and FQDN defined address objects to intelligently track dynamic IP/IP ranges.
- Must support NAT functionality, including NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT.
- Must support Combining source and destination NAT in the same policy
- May support Policy-based NAT and central NAT Table
- May supports provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP
- Must support Voice based protocols like H.323, SIP…etc.
- May support IPv6 for both NAT and Bridged Mode
- May support management over IPv6, IPv6 routing protocols, IPv6 tunneling, firewall and Threat Protection for IPv6 traffic, NAT46, NAT64, IPv6 IPSEC VPN
- Must support Inspection for SSL encrypted traffic option for IPS, application control, antivirus, web filtering, and DLP
- Must support Traffic redirection with ICAP and WCCP for Integration with existing solutions.
- Must support SSL MITM (Man in the middle) Mirroring
- Must support SSL Inspection Methods such as: SSL certificate inspection or full SSL inspection
- Must Support Network DLP to control shared files

4.3.6 HIGH AVAILABILITY

- Must support High availability modes: active-passive, active-active, clusters
- Must support High Availability between the virtual firewalls (Virtual Clustering).

- Must support state-full failover for both Firewall and VPN sessions.
- Must support Device Failure Detection and Notification as well as Link Status Monitor
- Must support VRRP and Link Failure Control

4.3.7 ROUTING & LOAD BALANCING

- Must support Link Aggregation Control Protocol
- Must Support SD-WAN
- Must support WAN Link LB algorithm, link status, plus quality checks, and policy routing support.
- Must Support Directing traffic among WAN links based on applications and users/user groups and IPsec VPN tunnels.
- Must support static and dynamic routing protocols
- Must support Policy based Routing
- Must support Dynamic routing protocols such as RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4
- Must support Multicast Routing
- May Support Traffic distribution across multiple backend servers based on multiple methods that account for different sized servers, or based on the health and performance of the server

4.3.8 APPLICATION CONTROL

- Must support granular application visibility and control and can detect based on behavior analysis not only service ports
- Must be able to Dynamically detect size of session to scan
- Must support granular application control such as allowing logins but not chatting over selected applications
- Must Support Granular user control for allowed applications access per single user or device /OS in a single policy
- Must support Custom application signature
- Must Support inspection of encrypted and evasive traffic, as well as traffic running on new technologies, such as SPDY protocol. The inspection can be applied to both network and IPsec/SSL VPN traffic.
- Must Support filter-based selection: By behavior, category, popularity, technology, risk, vendor, and/or protocol
- Must support Fine-grained control on popular cloud applications, such as Google Docs, and Dropbox.
- Must support IM applications control such as, Yahoo, Skype
- Must support Traffic shaping and QoS per applications
- Must Support SSH Inspection
- May Support customizable user notification for application violations

4.3.9 INTRUSION PREVENTION

- Must support a built-in Signature and Anomaly based IPS engine on the same unit
- Must support IPS regular and rate-based signatures, supported by zero-day threat protection and research for effective IPS implementation.

- Must support Filter-Based Selection by: Severity, target, OS, application, and/or protocol
- Must Support mitigation against Advanced Evasion Techniques such as IP Packet Fragmentation, TCP Stream Segmentation, RPC Fragmentation, URL & HTML Obfuscation
- Must Maintains up-to-date and proactive protection against latest known threats and newly discovered hacking techniques with real time & scheduled updates.
- Must support pre-defined action per IPS signature based
- Must Support IP Exemption for specific IPS signatures
- May Support Intrusion Detection mode (IDS Sniffer)
- Must support IPv4 and IPv6 rate-based DoS/DDoS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding.
- Must support attack quarantine capabilities
- May Support Packet logging for selected IPS signatures

4.3.10 AUTHENTICATION

- Must support both local and remote authentication services such as LDAP, Radius and TACACS+
- Must Support Single-Sign-On identity acquisition methods, including Windows AD, Terminal Servers, access portals, and mail services.
- Must support single sign-on capabilities to Windows AD, Citrix, or Novell eDirectory
- May support NTLM Authentication
- May support Radius single sign-on capabilities
- May support Certificate Based Authentication methods
- Must Support Implementing security policies through a combination of source objects, IPs, users, and/or devices.
- should support 2-factor authentication with In-built token server that manages both physical and mobile tokens for Admin & VPN access.

4.3.11 VISIBILITY, LOGGING & ANALYSIS

- Must support Real-time and historical threat status and network usage with comprehensive contextual information.
- Must support Physical and Logical topology pages
- Must support Dashboards with Customizable widgets that inform administrators of crucial system, licensing threats, and network status
- Support Endpoint Vulnerability Scanner chart
- Must support A variety of GUI consoles that display current and historical status using different perspectives such as ‘sources’, ‘destinations’, ‘interfaces’, ‘applications’, threats’ etc.
- Must support User notifications with customizable replacement message for blocked sites and attachments
- Must support Web Browser top banner insert showing application control violations, Endpoint control enforcement, web browsing quota etc
- Must support One-click remediation against listed source(s)/destination(s) for quick protection against threats and abuses.

- Must support Logging facilities on Local memory & storage.
- Must support integration with syslog servers.
- Must support Periodical system configuration check using a pre-defined PCI compliance checklist.
- May Support interconnection with other existing solution to provide best protection against the most advanced security threats and targeted attacks
- Must support config review for interconnected solutions against industry best practices

4.3.12 ENDPOINT VPN AGENT

- 100 VPN agent's license are required.
- Must contain and support the following components at least:
    - ✓ IPSEC/VPN client
    - ✓ SSL/VPN client
    - ✓ Native 2 factor Authentication
    - ✓ Must be able to integrate with offered Firewall and send data about the endpoint to it for better security policy control
    - ✓ User identification
    - ✓ Device details: IP address, MAC address, OS, etc…..
    - ✓ Security info such as vulnerabilities, malware detection, etc.
- Can provide WAN optimization for following protocols:
    - ✓ CIFS
    - ✓ FTP
    - ✓ HTTP
    - ✓ MAPI
    - ✓ General TCP traffic
- admin must be able to manage and monitor on-premises and off-premises clients.
- admin must be able to integrate with windows domain controller/active directory to client agent installation to all endpoints

4.3.13 SFPS:

The following number of SFPs are required and can be negotiated with the vendor according to National Operation Center (NOC) needs and design changes:

10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots	16
1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots	16

4.4 Security and Compliance

- The Bidder /OEM Should ensure necessary security features are built into the proposed **Internet Firewall solution**.
- The Bidder /OEM is responsible for remediation of cybersecurity vulnerability on software and hardware with no additional cost to National Operation Center (NOC)

- The Bidder /OEM is responsible for Implementation of security measures and policies in alignment with ISO, PCI-DSS, and other relevant compliance standards.
- The Bidder /OEM is responsible for Configuration of integrated security features such as encryption, access controls, and advanced threat protection.
- The Bidder /OEM Should ensure necessary compliance and security hardening as per National Operation Center (NOC) policies/requirements and submitting recommendations for further improvements to mitigate any possible threats, effective compliance check, better visibility and controls, etc.

4.5 Training and Documentation

- The Bidder /OEM Should Ensuring a smooth handover with detailed documentation and training provided to the National Operation Center (NOC) IT team.
- Installation and Configuration Documentation (documentation shall include screenshots for steps performed). Standard Operating Procedures (SOP) to be provided for **Internet Firewall solution**.
- The bidder/OEM shall provide a detailed drawing of the installed setup after completion of the project. This will also include the printout of important configuration settings of the solution.
- The OEM should provide a detailed architecture of the provided solution along Installation and Administration guide which must include High-level Design (HLD) and Low-Level Design (LLD).
- **Internet Firewall solution** diagram.
- detailed BOQ for proposed **Internet Firewall solution**.
- separate sheet for specification/white paper of the products.

4.6 Project Reporting and Handover

- Submission of commissioning reports detailing the deployment and configuration of the **Internet Firewall solution**.
- Provision of a comprehensive project completion report summarizing all activities, configurations, and outcomes.

4.7 Maintainability and Warranty Support

The scope under warranty shall cover to provide services as described below:

All delivered items Hardware and System software in this tender should be monitored and serviced in such a manner to ensure maximum uptime and performance levels. The guarantee/warranty should be

of the highest nature extended by the OEM on the date of participation in the Tender (Necessary documentary evidence to be submitted).

4.7.1 MAINTAINABILITY

- The Bidder will have to submit an undertaking from OEM assuring the availability of requisite spare parts for hardware (if any) the maintainability period of 5 (five) years from the date of installation.

- The software & hardware quoted by the bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 5 years of the Purchase order/contract period. In the event of the supplied equipment being declared End of Support/End of Life during the contract period of 5 (five) years, the bidder must replace the equipment with equipment having an equivalent or higher model.

4.7.2 WARRANTY SUPPORT

- Original Equipment Manufacturer (OEM) should have online 24 x 7 support for any hardware or software-related issue. The proposed solution should have one window support solution for all the components including hardware, firmware, and software used. The support should be from OEM.

- **Internet Firewall solution** must have direct OEM, L1, L2, and L3 support, 24x7x365 days with unlimited incident support (Telephonic / Web / Email) and technical contacts/contract within 4-hour response time including unlimited upgrades and updates during the tender specific warranty period.

- Provide on-site comprehensive warranty for the supplied items - equipment/system/subsystems (hardware and system software) for a period of 3 (three) years with 24x7 x 365 remote support and maximum resolution of NBD. The hardware equipment (if any) should be guaranteed/warranted against all defects and failure and such guarantee/warranty shall include replacement of defective parts/equipment and/or repair of the same free of cost. All warranty shall be onsite. The bidder should confirm in their response that the support during the warranty period would be carried out by the OEM for the respective equipment / peripheral. The bidder should also ensure that the SLA (24 x 7 x 365 support with a maximum resolution time of NBD) is adhered to, and this must be articulated in the bid response as well. The warranty shall also cover the following:

    i) Installation / re-installation / maintenance / reconfiguration of System software and other supplied software

    j) All system patches, upgrades, service packs, etc. of the OS and all other software supplied must be made available free of charge.

    k) Support for integration and update of infrastructure/network configuration and change management of the entire solution (existing as well as that procured as the scope of this tender) to meet business requirements.

l) Any change in the IP scheme, if required, limited to all the equipment installed at the Data Centre should be done in consultation with the National Operation Center (NOC) IT team.

- The non-delivery of services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP.
- In case of item replacement with a new one, the new item must be at least the same model, and in case the replacement is a higher model must be compatible with the National Operation Center (NOC). environment and technically approved by National Operation Center (NOC).

4.8 UPGRADES AND UPDATES

- The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Appliance/hardware & software provided free of charge during the contract period. If, however, the upgrades/updates are not available then the support for the implemented Solution/ Appliance/hardware & software should be available at any point of time. The solution (software or hardware or both) provided by the successful bidder should not be declared end of sale within 3 years of sign-off of the project. If at all the solution (software or hardware or both) is declared end of sale within 3 years of sign-off, the successful bidder must provide the upgraded version (software or hardware or both) free of charge, to the National Operation Center (NOC).
- The solution should provide seamless upgrades for (but not limited to) Firmware, software, BIOS, and other such functions which are required in the solution. All patches for the complete hardware and software solution must come from a single validated source. It should be possible to apply and upgrade all software and hardware-related firmware and patches from the same GUI that is used to manage the **Internet Firewall solution**.

4.9 Additional Consideration

Payment terms per project - 25% advance payment against non-conditional LG, 25% against delivery of Items, 40% after final commissioning & signoff -10% retention until end of the warranty period.

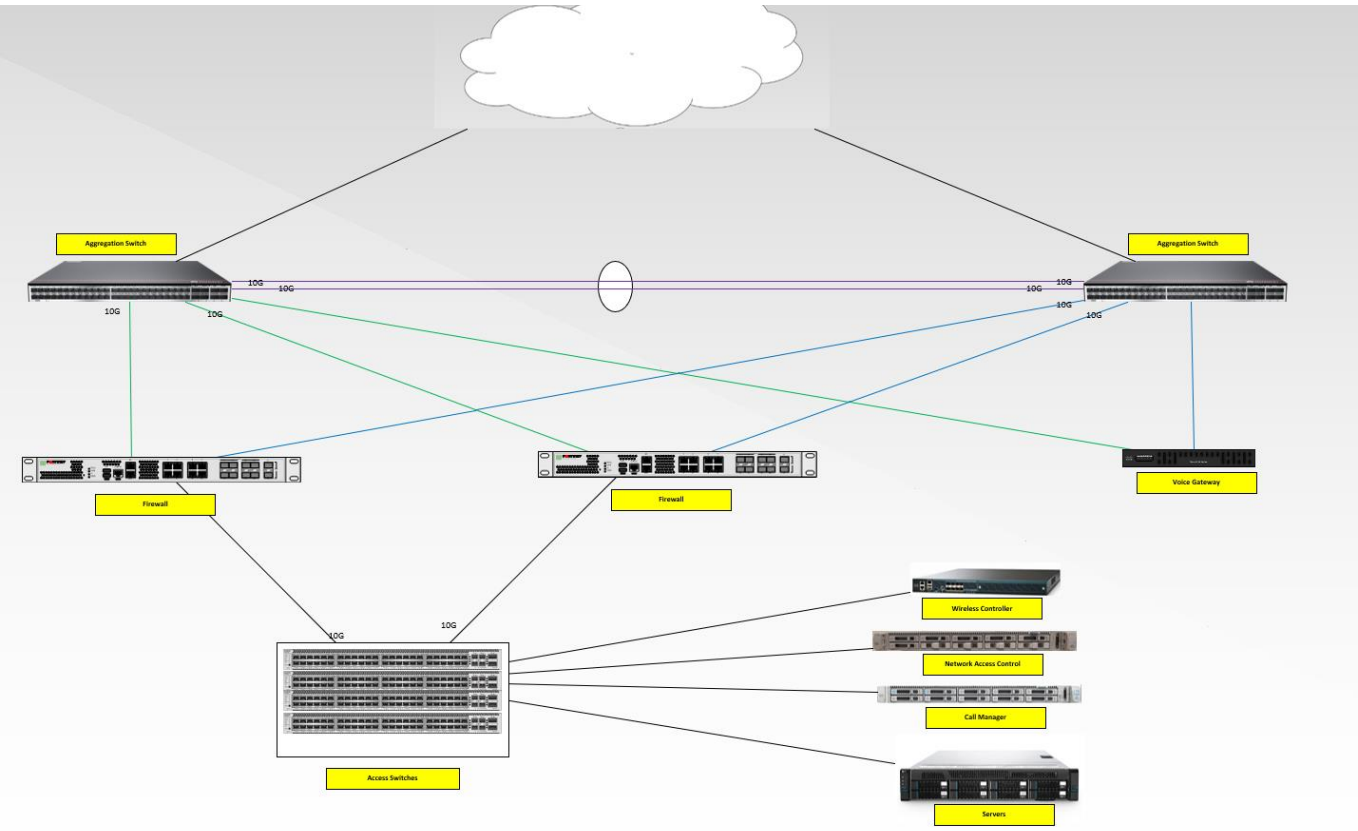
4.10 Levels of Service

The Supplier’s goal must be to meet, and even exceed, when possible, the levels of service described.

5 NETWORK SOLUTION

5.1 PURPOSE OF THE PROJECT:

The purpose of this RFP is to invite technically and commercially competitive proposals from reputed manufacturers/authorized representatives for **Network solution**. The vendor engagement will involve Supply, Installing, Configuring, Testing, Implementing, and Commissioning of the new solution, as well as providing incident and product support as per Scope of work and Technical Specifications given in this RFP, at National Operation Center (NOC) Datacenter.



5.2 SCOPE of work

- The broad scope of work as detailed in this section refers to the Hardware and System software for internet firewall that is procured through this tender and used for Supply, Installing, Configuring, Testing, Implementing, and Commissioning of the **Network solution** at National Operation Center (NOC).

- **Licensing Coverage**: The bidder/OEM must ensure that all necessary licenses for the **Network solution** are fully covered.
- **Responsibility for Additional Licenses**: If any licenses needed to complete the solution are identified after the proposal is submitted, the bidder/OEM will be responsible for covering the costs of those additional licenses.

- **this scope of work shall include, but not be limited to, the following:**

5.2.1 GENERAL CONDITIONS

- Professional Services are requested for complete & full implementation and configuration for **Network solution** in National Operation Center (NOC).
    - The OEM/bidder shall be responsible for Design, Supply, Installation, Configuration, Testing and Commissioning of the **Network solution** in at National Operation Center (NOC).
    - The OEM shall be doing the Project Management for the entire Project from commencement to final handing over for live use. The proposed solution must be supported for a period of 3 years as per RFP and National Operation Center (NOC) requirement.
    - The OEM must prepare architecture design, optimize network to increase performance, documentation, project plan and training as part of the implementation services.
    - Installation and configuration of supplied hardware associated system software and system integration must be carried out by OEM or authorize partner.
    - Bidder/OEM should propose highly scalable solution. Solutions with limited scalability would not be acceptable to National Operation Center (NOC). Solutions which are not mature for over 1 year should not be quoted.
    - The Bidder/OEM shall be responsible for performing the necessary changes in the configuration required for Hardening and/or request directed by security team & audit team.
    - The Bidder/OEM shall be responsible for firmware patches/bug, fixes BIOS upgrade and Version Upgrade of software.
    - The Bidder/OEM shall be responsible for generation and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams and other reports etc. All such documents shall commence only after the same is approved by National Operation Center (NOC).
    - The Bidder/OEM should provide a detailed project plan in terms of activity and phase-wise timelines (no. of days) required for executing the project with the details of deliverables and milestones including the delivery of Network Solution components. The Bidder/OEM shall inform the name of the Project Manager who would be the single point of contact during the complete project implementation.
    - The OEM must analyze, review, and gather performance metrics and ensure it performs optimally.

- The Bidder/OEM shall be responsible for installing / configuring of all patches / updates / upgrades required for the offered solution without any extra cost to National Operation Center (NOC) during the warranty period.
- All service requests for **Network solution** should be received, managed, executed, and tracked to closure by the OEM or through Authorized Service Provider.
- All related documents, manuals, catalogues, and information furnished by the bidder shall become the property of the National Operation Center (NOC). Detailed process documentation, and SOP‟s (Standard Operating Procedure) should be submitted before project signoff.
- National Operation Center (NOC) may opt for Audit through a third party Authorized Agency or by the Terminal officials for the supplied hardware and Software. Successful bidder is required to coordinate with the Terminal Officials& Audit agency execute relevant test cases.
- National Operation Center (NOC) will have a periodic review of technology. Successful bidder will supply the models approved as per technical aspects. In case any of the models becomes end of support during entire contract period, then Successful bidder will provide the latest model available at no extra cost to National Operation Center (NOC) without disruption in performance of services/applications.
- During the Contract Period, in case there is hardware failure three or more times in a period of less than three (3) months, then it shall be replaced by equivalent or higher-level new equipment by the Successful bidder at no cost to the National Operation Center (NOC).
- The Bidder/OEM must Proposed a scalable, turnkey **network solution**

5.2.2 DELIVERY ACCEPTANCE TEST

- All the delivered hardware items may be subjected to an acceptance test. Successful bidders must arrange one Engineer at the site at the date and time mentioned by the National Operation Center (NOC) to assist in the acceptance test.
- The successful bidder shall submit test report. The report should include the below contents:
    a. Test case
    b. Test case description
    c. Expected result
    d. Actual result
    e. Pass / fail
    f. Screen capture of the result

5.2.3 SUPPLY AND DEPLOYMENT

- The accessories of **network solution** (including cables, rack mounting kit, Power strip in the rack etc.) required for the installation and configuration of the equipment will also be supplied by the successful Bidder.
- The Successful Bidder is responsible for all materials like SFP /Ethernet modules cables, connectors etc., equipment's, and services, specified or otherwise.
- The bidder shall be responsible for delivery and installation of the complete **network solution** ordered at National Operation Center (NOC) requirement. Installation means mounting of **network solution** in Rack (If any) and "Power-On" all the hardware with all the accessories provided with the hardware.
- The Successful Bidder is responsible for all unpacking and shall carry out the installation, commissioning, and configuration of all the hardware & appliances and related software as required during the installation.
- The selected bidder should provide a full proof project execution plan before implementing the solution. The project execution plan should be without any network security breach.
- The project should roll out as per execution plan upon approval from the National Operation Center (NOC) IT management.
- The supply and installation of ordered items along with necessary setup, operational and user manuals / drawings, hardening guide, system test report, circuit diagram, if any etc., shall be made available and handed over to National Operation Center (NOC) Unit after installation.
- The Bidder shall 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 be provisioned according to the requirements of the solution.
- The bidder shall provision for any components, subcomponents, assemblies, subassemblies as part of the **network solution** in the bid response. In case the bidder has not provisioned for the above, the same shall be provisioned to meet solution requirements at no additional cost and time implications to the purchaser.
- The testing of all equipment & appliances and its operations shall be the responsibility of successful bidder and its OEM. They shall also accomplish all adjustments necessary for successful and continuous operation of these Hardware's and software's supplied, installed & commissioned under this tender.

5.2.4 CONFIGURATION AND COMMISSIONING

- The Successful Bidder shall be responsible for commissioning of the items supplied by preparing interfacing / integrating with purchaser's equipment / accessories / supplied by other vendors Integration and configuration of the **network solution** as per the compliance sheet and international best practices.

- OEM will be responsible for Install and configure **network solution**, including all necessary licenses.

- **Acceptance Criteria of Commissioning**

1. **Physical Inspection**:
    a. Verify that all network solution is installed in the correct locations and are securely mounted.
    b. Check that all cables are properly connected and labeled according to the network design.
2. **Power and Connectivity**:
    a. Ensure that each network solution powers on correctly and that all power supplies are functioning.
    b. Confirm that all network ports are operational and can establish connections with other network devices.
3. **Configuration Verification**:
    a. Validate that the switch configuration matches the network design specifications, including VLANs, IP addresses, and routing protocols.
    b. Check that security settings, such as access control lists (ACLs) and port security, are correctly implemented.
4. **Performance Testing**:
    a. Conduct performance tests to ensure the switch can handle the expected network traffic without issues.
    b. Test for latency, throughput, and packet loss to verify network performance under load.
5. **Redundancy and Failover**:
    a. Test redundancy features such as link aggregation, spanning tree protocol (STP), and redundant power supplies.
    b. Ensure that failover mechanisms work correctly and that the network remains operational in case of a failure.
6. **Security and Compliance**:
    a. Verify that the network solution complies with all relevant security policies and standards.
    b. Conduct vulnerability assessments to identify and mitigate potential security risks.

5.3 Technical Specification / Requirement

5.3.1 ACCESS SWITCHES

Technical specifications of the switches as the following:

General Technical specs

● All devices must be delivered with two redundant power supply.

● Flexible and dense fiber uplink offerings with 1G, Multigigabit, 10G in the form of fixed or modular uplinks.

● Flexible downlink options with 1G,5G,10G Copper and Fiber as well as the densest Multigigabit links

● IPv6 support in hardware, providing wire-rate forwarding for IPv6 networks

● Dual-stack support for IPv4/IPv6 and dynamic hardware forwarding table allocations, for ease of IPv4-to-IPv6 migration

● Dual-stack support for IPv4 and dynamic hardware forwarding table allocations up to 5 switches.

● Support PoE capabilities, POE & PoE+.

● Plug and Play (PnP) enabled: A simple, secure, unified, and integrated offering to ease new branch

● Support for IEEE802.1x authentication.

● IEEE 802.1Q (VLAN Tagging).

● IEEE 802.1D (Spanning Tree Protocol).

Advanced security that must be available in the switches:

● Encrypted Traffic Analysis: is the capability for identifying malware in encrypted traffic coming from the access layer.

● AES-256 MACsec encryption is the IEEE 802.1AE standard for authenticating and encrypting packets between switches.

● Hardware and software authenticity: switching solution support trust and strong mitigation against man-in-the-middle attacks that compromise software and firmware. Like the following

● Image signing: Cryptographically signed images provide assurance that the firmware, BIOS, and other software are authentic and unmodified.

● Firmware Boot sequence Security: to provides layered protection against the persistence of illicitly modified firmware.

● Hardware authenticity assurance to uniquely identify the product and provides assurance that the product is genuine.

● DNS Security Integration: This allows the business to easily customize their DNS filtering policies granularly at user or group level to prevent BYOD or IoT guest or corporate users from accessing malicious or inappropriate websites.

High availability:

The switches must support the below high-availability features:

● Ability to configure aggregated interfaces technology across different members of the stack for high resiliency with stack cables.

● IEEE 802.1AX (Link Aggregation).

● IEEE 802.3ad

● IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP).

●IEEE 802.1w RSTP.

● Non-Stop data Forwarding must be supported to reduce traffic downtime during switchover times.

● The following number of switches is required (All below switches must full fill all above the technical specs)

Switch Role	Description	
Aggregation Switches	48-port 1G copper with 8x10G SFP+ uplinks, data only	2
Access Switches 48 Ports multi-gig support	48-Port with multi-gig features support 8x10G Uplink, PoE+ on all ports	4
SFP 10G	Multi-Mode Short Range	16
SFP 1G	Multi-mode Mode Long Range	8
Fiber patch cord LC-LC	Multi-Mode fiber patch cord LC-LC 5 M	20

5.3.2 NAC SOLUTION

The proposed NAC Solution should support below features:

- All devices shall be delivered with two redundant power supplies.
- The NAC solution can be a part of the of the security firewall solution.
- Must be from the same vendor of switches and wireless access points.
- Endpoint Classification & Visibility
  NAC should detect both new and existing endpoints and categorize them based on the type of endpoints (Ex: Windows, Linux/Unix, Printer, IP Cameras, smartphones, tablets such as Android/ IOS & Network Devices, etc.).
- Endpoint Profiling
  NAC should detect a new connection to the network and assess that it is not a device belonging to the corporate network or domain and handle the device Corporate and Guests as specified within the rule.
- Administrators can also create their device templates & can also associate endpoint-specific authorization policies based on device type. NAC should support downloadable Access Lists and URL redirection.
- L2 or L3 Deployment Option

The Clean Access Server can be deployed within L2 proximity of users, or multiple hops away from users.

- In-Band (IB) or Out-of-Band (OOB) deployment options
  NAC Appliance should be deployed in-line with user traffic, or out-of-band to allow clients to traverse the Clean Access network only during vulnerability assessment and remediation while bypassing it after certification (posture assessment).
- Endpoint Access Control
  NAC should completely block non-compliant / unknown users over wired. Wireless, VPN networks.
- Endpoint Remediation
  Redirection of non-compliant into quarantine segments and applying remediation policies.
- Multivendor Support
  The solution should support multi-vendor devices to provide greater intelligence and enhanced visibility.
- Multi Identity Support
  NAC should support multiple authentication and authorization sources including AD, LDAP, RADIUS, etc.
- Guest Management
  NAC should identify guest users and devices from registered users and devices and limit guest access based on defined policies.
- Alert Mechanism
  NAC should support email notifications with detailed and required information upon violation of defined policies.
- Reporting
  NAC dashboard should provide detailed reports that provide overall network endpoint visibility.

5.3.3 INDOOR WIRELESS SOLUTION

The proposed Wireless Solution should support below features:

- Must be from the same vendor of switches and NAC solution.
- Access points must have WIFI6 support and POE support.
- Can work as a standalone access point and can work with a wireless access point controller.
- Provides uplink speeds of 5.0 Gbps.
- support multiple SSID broadcasting
- support Wi-Fi roaming
- separate internal network traffic and guest network traffic (Internet access only), i.e., a WLAN for internal network and guest (Internet only) network respectively
- support various kinds of authentication methods such as 802.1x, MAC, Captive Portal (for guest users)
- The vendor must provide a heatmap that proves that the solution can well cover all the buildings including the number of the needed access points.

5.4 Security and Compliance

- The Bidder /OEM Should ensure necessary security features are built into the proposed network solution.
- The Bidder /OEM is responsible for remediation of cybersecurity vulnerability on software and hardware with no additional cost to National Operation Center (NOC)
- The Bidder /OEM is responsible for Implementation of security measures and policies in alignment with ISO, PCI-DSS, and other relevant compliance standards.
- The Bidder /OEM is responsible for Configuration of integrated security features such as encryption, access controls, and advanced threat protection.
- The Bidder /OEM Should ensure necessary compliance and security hardening as per National Operation Center (NOC) policies/requirements and submitting recommendations for further improvements to mitigate any possible threats, effective compliance check, better visibility, and controls, etc.

5.5 Training and Documentation

- The Bidder /OEM Should Ensuring a smooth handover with detailed documentation and training provided to the National Operation Center (NOC) IT team.
- Installation and Configuration Documentation (documentation shall include screenshots for steps performed). Standard Operating Procedures (SOP) to be provided for network solution.
- The bidder/OEM shall provide a detailed drawing of the installed setup after completion of the project. This will also include the printout of important configuration settings of the solution.
- The OEM should provide a detailed architecture of the provided solution along Installation and Administration guide which must include High-level Design (HLD) and Low-Level Design (LLD).
- detailed BOQ for proposed network solution.
- separate sheet for specification/white paper of the products.

5.6 Project Reporting and Handover

- Submission of commissioning reports detailing the deployment and configuration of the network solution.

- Provision of a comprehensive project completion report summarizing all activities, configurations, and outcomes.

5.7 Maintainability and Warranty Support

The scope under warranty shall cover to provide services as described below:

All delivered items Hardware and System software in this tender should be monitored and serviced in such a manner to ensure maximum uptime and performance levels. The guarantee/warranty should be of the highest nature extended by the OEM on the date of participation in the Tender (Necessary documentary evidence to be submitted).

5.7.1 MAINTAINABILITY

- The Bidder will have to submit an undertaking from OEM assuring the availability of requisite spare parts for hardware (if any) the maintainability period of 5 (five) years from the date of installation.
- The software & hardware quoted by the bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 5 years of the Purchase order/contract period. In the event of the supplied equipment being declared End of Support/End of Life during the contract period of 5 (five) years, the bidder must replace the equipment with equipment having an equivalent or higher model.

5.7.2 WARRANTY SUPPORT

- Original Equipment Manufacturer (OEM) should have online 24 x 7 support for any hardware or software-related issue. The proposed solution should have one window support solution for all the components including hardware, firmware, and software used. The support should be from OEM.
- **network solution** must have direct OEM, L1, L2, and L3 support, 24x7x365 days with unlimited incident support (Telephonic / Web / Email) and technical contacts/contract within 4-hour response time including unlimited upgrades and updates during the tender specific warranty period.
- Provide on-site comprehensive warranty for the supplied items - equipment/system/subsystems (hardware and system software) for a period of 3 (three) years with 24x7 x 365 remote support and maximum resolution of NBD. The hardware equipment (if any) should be guaranteed/warranted against all defects and failure and such guarantee/warranty shall include replacement of defective parts/equipment and/or repair of the same free of cost. All warranty shall be onsite. The bidder should confirm in their response that the support during the warranty period would be carried out by the OEM for the respective equipment / peripheral. The bidder should also ensure that the SLA (24 x 7 x 365 support with a maximum resolution time of NBD) is adhered to, and this must be articulated in the bid response as well. The warranty shall also cover the following:

    m) Installation / re-installation / maintenance / reconfiguration of System software and other supplied software

n) All system patches, upgrades, service packs, etc. of the OS and all other software supplied must be made available free of charge.

o) Support for integration and update of infrastructure/network configuration and change management of the entire solution (existing as well as that procured as the scope of this tender) to meet business requirements.

p) Any change in the IP scheme, if required, limited to all the equipment installed at the Data Centre should be done in consultation with the National Operation Center (NOC) IT team.

- The non-delivery of services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP.
- In case of item replacement with a new one, the new item must be at least the same model, and in case the replacement is a higher model must be compatible with the National Operation Center (NOC) environment and technically approved by National Operation Center (NOC)

5.8 UPGRADES AND UPDATES

- The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Appliance/hardware & software provided free of charge during the contract period. If, however, the upgrades/updates are not available then the support for the implemented Solution/ Appliance/hardware & software should be available at any point of time. The solution (software or hardware or both) provided by the successful bidder should not be declared end of sale within 3 years of sign-off of the project. If at all the solution (software or hardware or both) is declared end of sale within 3 years of sign-off, the successful bidder must provide the upgraded version (software or hardware or both) free of charge, to the National Operation Center (NOC).
- The solution should provide seamless upgrades for (but not limited to) Firmware, software, BIOS, and other such functions which are required in the solution. All patches for the complete hardware and software solution must come from a single validated source. It should be possible to apply and upgrade all software and hardware-related firmware and patches from the same GUI that is used to manage the **Internet Firewall solution**.

5.9 Additional Consideration

Payment terms per project - 25% advance payment against non-conditional LG, 25% against delivery of Items, 40% after final commissioning & signoff -10% retention until end of the warranty period.

5.10 Levels of Service

The Supplier's goal must be to meet, and even exceed, when possible, the levels of service described.

6 SERVERS & RACKS

6.1 PURPOSE OF THE PROJECT:

The purpose of this RFP is to invite technically and commercially competitive proposals from reputed manufacturers/authorized representatives for **Servers & Racks.** The vendor engagement will involve Supply, Installing, Configuring, and Testing of the new hardware, as well as providing incident and product support as per Scope of work and Technical Specifications given in this RFP, at National Operation Center (NOC) Datacenter.

6.2 SCOPE of work

- The broad scope of work as detailed in this section refers to the servers (Hardware, firmware) and Racks that is procured through this tender and used for Supply, Installing, and Testing of the **2 Servers and 2 racks at** National Operation Center (NOC).
- **this scope of work shall include, but not be limited to, the following:**

6.2.1 GENERAL CONDITIONS

- Servers OEM should be from Leader's quadrant of Gartner's report
- The OEM/bidder shall be responsible for Supply, Installation, and Testing of the **Servers** in Racks at National Operation Center (NOC).
- The proposed servers must be supported for a period of 3 years as per RFP and National Operation Center (NOC) requirement.
- The Bidder/OEM shall be responsible for firmware patches/bug, fixes BIOS upgrade and Version Upgrade of software.
- During the Contract Period, in case there is hardware failure three or more times in a period of less than three (3) months, then it shall be replaced by equivalent or higher-level new equipment by the Successful bidder at no cost to the National Operation Center (NOC).

6.2.2 DELIVERY ACCEPTANCE TEST

- All the delivered hardware items may be subjected to an acceptance test. Successful bidders must arrange one Engineer at the site at the date and time mentioned by the National Operation Center (NOC) to assist in the acceptance test.
- The successful bidder shall submit test report. The report should include the below contents:
    a. Test case
    b. Test case description
    c. Expected result
    d. Actual result
    e. Pass / fail
    f. Screen capture of the result

6.2.3 SUPPLY AND DEPLOYMENT

- The accessories of **Servers and Racks** (including cables, rack mounting kit, Power strip in the rack, Smart PDU etc.) required for the installation and configuration of the equipment will also be supplied by the successful Bidder.
- The Successful Bidder is responsible for all materials like Ethernet cables, racks organizer etc., equipment's, and services, specified or otherwise.
- The bidder shall be responsible for delivery and installation of the complete servers and Racks ordered at the National Operation Center (NOC) requirement. Installation means mounting of **Servers** in Rack (If any) and "Power-On" all the hardware with all the accessories provided with the hardware.

- The Bidder shall 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 be provisioned according to the requirements of the solution.
- The bidder shall provision for any components, subcomponents, assemblies, subassemblies as part of the **Servers and Racks** in the bid response. In case the bidder has not provisioned for the above, the same shall be provisioned to meet solution requirements at no additional cost and time implications to the purchaser.
- The testing of all equipment and its operations shall be the responsibility of successful bidder and its OEM. They shall also accomplish all adjustments necessary for successful and continuous operation of these Hardware's and software's supplied, installed under this tender.

6.3 Technical Specification / Requirement

6.3.1 SERVERS-QTY (2):

Management Server - Main Configuration	QTY
Intel Xeon Silver 4310 2.1G, 12C/24T, 10.4GT/s, 18M Cache, Turbo, HT (120W) DDR4-2666 & Heatsink for CPU	2
16GB RDIMM, 3200MT/s, Dual Rank	4
SAS/SATA Backplane	1
Raid Controller support Raid1 & Raid5	1
480GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug (RAID 1)	2
960GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug (RAID 5)	4
Quad Port 1GbE BASE-T Adapter	1
Integrated Remote Access Controller	1
Trusted Platform Module 2.0 V3	1
Dual, Hot-plug, PSU (1+1)	1
No Operating System	1
Warranty 3 years	1
Domain Controller Server - Main Configuration	**QTY**
Intel Xeon Silver 4310 2.1G, 12C/24T, 10.4GT/s, 18M Cache, Turbo, HT (120W) DDR4-2666 & Heatsink for CPU	2
16GB RDIMM, 3200MT/s, Dual Rank	4
SAS/SATA Backplane	1
Raid Controller support Raid1	1
960GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug (RAID 1)	2
Quad Port 1GbE BASE-T Adapter	1
Integrated Remote Access Controller	1

Trusted Platform Module 2.0 V3	1
Dual, Hot-plug, PSU (1+1)	1
No Operating System	1
Warranty 3 years	1

6.3.2 RACKS-QTY (2):

- 42U Server Rack include enclosure fans, Blanking Panels / Filler Panels, and cable management accessories
- 2 smart PDUs, with 16 outlets and 32A
- Rackspace: 42 U
- Maximum Depth for Equipment (mm): 850
- Swing handles with key lock.
- four infinitely adjustable 19” mounting rails with U-markings
- Plain top panel with two cover plates for optional airflow or cable management brush inserts
- Air Ventilation: Air enters from the front door and exhausts from the rear door.
- Front door - perforated
- Door Perforation Rate: ≥80%
- Door Structure: Front single door and rear double doors with a 140o opening angle.
- Rear door - perforated (perforated model)
- Sides Removable, lockable side panels - on models with sides.
- Regulatory approvals & standards EIA-310-E, IEC / EN 60950, IEC / EN 60297, IEC 529
- Static Load: 2400kg
- Fan set with 4 fans and thermostat suitable for 800mm deep server racks
- Casters and levelling feet
- Grounding kit
- Toolless 19-inch plastic cover panel – 1U (21 per rack)
- M6 cage nuts - set for 19-inch mounting (168 per rack)
- Extendible shelf for 800mm deep server racks - 1U (2 per rack)
- Dynamic Load: 1000
- Mount Bar Adjustment Step: The depth stride of the mounting bars is 25 mm. By default, the cabinet supports device installation with a depth of 750 mm to suit the mainstream and high-performance servers in the industry.
- Amount of Cabling: Supports150 network cables or 64 optical fibers on the right that are routed from the top of the cabinet.
- Cable management accessories should be included.
- Color Surface Finish: Black (PANTONE426C/RAL9005), Black surface with indoor powder-coat, meeting requirements for Class A environments.
- Material: High-intensity class A carbon cold rolled steel plate and zinc-coated steel plate.
- Protection Level: IP20

- Environmental Protection Compliance: RoHS

- Installation: Installed directly on an ESD floor, bracket, or concrete floor
- Rack must include Environmental Sensor like (heat, humidity, water sensors, etc.)
- Environmental Sensor should have Email Notification capability

6.4 Maintainability and Warranty Support

The scope under warranty shall cover to provide services as described below:

All delivered items Hardware and System software in this tender should be monitored and serviced in such a manner to ensure maximum uptime and performance levels. The guarantee/warranty should be of the highest nature extended by the OEM on the date of participation in the Tender (Necessary documentary evidence to be submitted).

6.4.1 MAINTAINABILITY

- The Bidder will have to submit an undertaking from OEM assuring the availability of requisite spare parts for hardware (if any) the maintainability period of 5 (five) years from the date of installation.

- The software & hardware quoted by the bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 5 years of the Purchase order/contract period. In the event of the supplied equipment being declared End of Support/End of Life during the contract period of 5 (five) years, the bidder must replace the equipment with equipment having an equivalent or higher model.

6.4.2 WARRANTY SUPPORT

- Original Equipment Manufacturer (OEM) should have online 24 x 7 support for any hardware or software-related issue. The proposed solution should have one window support solution for all the components including hardware, firmware, and software used. The support should be from OEM.

- **Servers** must have direct OEM, L1, L2, and L3 support, 24x7x365 days with unlimited incident support (Telephonic / Web / Email) and technical contacts/contract within 4-hour response time including unlimited upgrades and updates during the tender specific warranty period.

- Provide on-site comprehensive warranty for the supplied items - equipment/system/subsystems (hardware and system software) for a period of 3 (three) years with 24x7 x 365 remote support and maximum resolution of NBD. The hardware equipment (if any) should be guaranteed/warranted against all defects and failure and such guarantee/warranty shall include replacement of defective parts/equipment and/or repair of the same free of cost. All warranty shall be onsite. The bidder should confirm in their response that the support during the warranty period would be carried out by the OEM for the respective equipment / peripheral. The bidder should also ensure that the SLA (24 x 7 x 365 support with a maximum resolution time of NBD) is adhered to, and this must be articulated in the bid response as well. The warranty shall also cover the following:

q) Installation / re-installation / maintenance / reconfiguration of System software and other supplied software

r) All system patches, upgrades, service packs, etc. of the OS and all other software supplied must be made available free of charge.

s) Support for integration and update of infrastructure/network configuration and change management of the entire solution (existing as well as that procured as the scope of this tender) to meet business requirements.

t) Any change in the IP scheme, if required, limited to all the equipment installed at the Data Centre should be done in consultation with the National Operation Center (NOC) IT team.

- The non-delivery of services or non-response or any breach of information will lead to penalty. The penalty is applicable in respect of non-delivery of services/ support as per the requirement of this RFP.
- In case of item replacement with a new one, the new item must be at least the same model, and in case the replacement is a higher model must be compatible with the National Operation Center (NOC). environment and technically approved by National Operation Center (NOC)

6.5 UPGRADES AND UPDATES

- The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Appliance/hardware & software provided free of charge during the contract period. If, however, the upgrades/updates are not available then the support for the implemented Solution/ Appliance/hardware & software should be available at any point of time. The solution (software or hardware or both) provided by the successful bidder should not be declared end of sale within 3 years of sign-off of the project. If at all the solution (software or hardware or both) is declared end of sale within 3 years of sign-off, the successful bidder must provide the upgraded version (software or hardware or both) free of charge, to the National Operation Center (NOC).
- The solution should provide seamless upgrades for (but not limited to) Firmware, software, BIOS, and other such functions which are required in the solution. All patches for the complete hardware and software solution must come from a single validated source. It should be possible to apply and upgrade all software and hardware-related firmware and patches from the same GUI that is used to manage the **Servers.**

6.6 Additional Consideration

Payment terms per project - 25% advance payment against non-conditional LG , 25% against delivery of Items, 40% after final commissioning & signoff -10% retention until end of the warranty period.

6.7 Levels of Service

The Supplier's goal must be to meet, and even exceed, when possible, the levels of service described.

7 TIME ATTENDANCE MACHINE

7.1 PURPOSE OF THE PROJECT:

The purpose of this RFP is to invite technically and commercially competitive proposals from reputed authorized representatives for **time attendance machine.** The vendor engagement will involve Supply, Installing, Configuring, and Testing of the new hardware, as well as providing incident and product support as per Scope of work and Technical Specifications given in this RFP, at National Operation Center (NOC) Datacenter.

7.2 SCOPE of work

- The broad scope of work as detailed in this section refers to the **Morpho attendance machines** (Hardware, firmware) that is procured through this tender and used for S supply, install, and configure Morpho attendance machines with existing Morpho Manager software already exist in production environment in another site for National Operation Center (NOC).
- **this scope of work shall include, but not be limited to, the following:**

7.21 GENERAL CONDITIONS

- POC of Morpho attendance machines is required from bidder to ensure compatibility with existing Morpho Manager software and existing employee biometric figure template exist in Morpho manager database.
- Installing and configuring Morpho attendance machines in respective location with all needed accessories for installation that must be delivered by supplier.
- Delivering and installing required network cable and guaranty network reachability for attendance machines.
- Provide HW Warranty 3 years for Morpho attendance machines including the replacement of defected devices and starting next business day of project sign off.

- Repair will be on site and the vendor must have and deliver all material needed to repair or replace the defective part.
- Response time within working hours with ticket number and resolution next business day and close the ticket with technical report.
- The hardware quoted by bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the vendor within the 5 years of Purchase order / contract period. In the event of the supplied equipment being declared End of support/End of Life during the contract period of five years, the bidder must replace the equipment with equipment having equivalent or higher configurations.
- NOC may opt for Audit through a third party Authorized Agency or by the Terminal officials for the supplied hardware, Successful bidder is required to coordinate with the Terminal Officials& Audit agency execute relevant test cases and solve any security remark related to security scan result.
- In case of item replacement with new one, the new item must be at least same model, and in case the replacement is higher model, it must be compatible with existing environment and technically approved by IT team.

7.2.2 DELIVERY ACCEPTANCE TEST

- All the delivered hardware items may be subjected to an acceptance test. Successful bidders must arrange one Engineer at the site at the date and time mentioned by the National Operation Center (NOC) to assist in the acceptance test.
- The successful bidder shall submit test report. The report should include the below contents:

g. Test case
h. Test case description
i. Expected result
j. Actual result
k. Pass / fail
l. Screen capture of the result

7.2.3 SUPPLY AND DEPLOYMENT

- The Successful Bidder is responsible for all materials like Ethernet cables, racks organizer etc., equipment's, and services, specified or otherwise.
- The Bidder shall 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 be provisioned according to the requirements of the solution.

7.3 Technical Specification / Requirement

7.3.1 ATTENDANCE MACHINES REQUIREMENT: QTY (4)

- Full support and compatibility between delivered attendance machines and existing Morpho Manager attendance software in another site with existing employee biometric figure template in Morpho manager database.
- Morpho Attendance machines should clearly indicate the successful and failure status of the employee transaction physically on the machine in real time.
- Ability to recover employee biometric transaction logs with no data loss on the defected attendance machined which not pulled with Morpho attendance application.
- The attendance machine must accept the employee finger biometric or access card ID and store the transaction locally in case the attendance application is offline and when the application become online the transaction have been pulled automatically from the machines without data loss.
- Morpho attendance machine must support POE.
- Attendance machines can identify the employee biometric type in all environmental cases (High and low light, dust, etc.).
- vendor Should ensure necessary security features are built into the proposed attendance machine.
- The attendance machine must have the ability to check employee profile including finger biometric or access card type during transaction from internal attendance machine database without connecting attendance software.
- Attendance machine must have the ability to authenticate employee against finger biometric and card ID.
- Attendance machine must have High capacity with min. 3,000 employee profile each one can include all attend type (two finger biometric (one in each hand) and card ID and min. 100,000 logs.
- Attendance machine must have the capability to expand capacity (Number of employee profiles) without replace it.
- Fast matching in 1 to many modes between employee and attendance machine.
- Anti-fraud: fake finger, duress finger.
- Attendance machine must be certified with IP65 rated, IP66 preferred.
- Attendance machine must have ethernet port for network connection and communication with attendance software.
- Attendance machine will be designed to be used for Check-In or Check-Out not both and based on machine ID the employee transaction will be send to Morpho attendance software as check in if it configured as Check In machine or Check Out if it configured as Check Out no selection from employee site.

7.3.2 FINGERPRINT ENROLLMENT DESKTOP SCANNER: QTY (1)

- Morpho Smart Fingerprint Enrollment Desktop Machine for HR operator to take employee biometric finger and deploy it to attendance software.

7.4 Additional Consideration

Payment terms per project - 25% advance payment against non-conditional LG , 25% against delivery of Items, 40% after final commissioning & signoff -10% retention until end of the warranty period.

7.5 Levels of Service

The Supplier's goal must be to meet, and even exceed, when possible, the levels of service described.

8 APC-SMARTUPS-ONLINE-8KVA

8.1 PURPOSE OF THE PROJECT:

The purpose of this RFP is to invite technically and commercially competitive proposals from reputed authorized representatives for **apc-smartups-online-8kva.** The vendor engagement will involve Supply, Installing, Configuring, implementing, commissioning, and Testing of the new UPS, as well as providing incident and product support as per Scope of work and Technical Specifications given in this RFP, at National Operation Center (NOC) Datacenter.

8.2 SCOPE of work

- The broad scope of work as detailed in this section refers to the **apc-smartups-online-8kva** that is procured through this tender and used for Supply, Installing, Configuring, implementing, commissioning, and Testing of the new UPS in National Operation Center (NOC) Data Center.
- **this scope of work shall include, but not be limited to, the following:**

7.21 GENERAL CONDITIONS

- Installing and configuring **apc-smartups-online-8kva** in respective location with all needed accessories for installation that must be delivered by supplier.
- Delivering and installing required electric cables for UPS.
- Provide HW Warranty 3 years for **apc-smartups-online-8kva** including the replacement of defected devices and starting next business day of project sign off.
- The bidder shall offer on-site comprehensive warranty (including hardware and software) for UPS
- OEM Warranty certificates must be submitted by Successful Bidder at the time of delivery of Goods. The seller should guarantee the rectification of goods in case of any break down during the guarantee period. Seller should have well established Maintenance Service facility for attending the after sales service.
- Repair will be on site and the vendor must have and deliver all material needed to repair or replace the defective part.
- Response time within working hours with ticket number and resolution next business day and close the ticket with technical report.
- The hardware quoted by bidder in this RFP should not be declared as End of Life (EOL) or End of Support (EOS) by the vendor within the 5 years of Purchase order / contract period. In the event of the supplied equipment being declared End of support/End of Life during the contract period of five years, the bidder must replace the equipment with equipment having equivalent or higher configurations.

7.2.2 SUPPLY AND DEPLOYMENT

- The Successful Bidder is responsible for all materials., equipment's, and services, specified or otherwise.
- The Bidder shall 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 be provisioned according to the requirements of the solution.

8.3 Technical Specification / Requirement

8.3.1 ATTENDANCE MACHINES REQUIREMENT: QTY (1)

ITEM	Part Number
• **apc-smartups-online-8kva-8kw-tower-230v-31-and-11-6x-c13+4x-c19-iec-outlets-network-card+smartslot-extended-runtime-w-o-rail-kit**	• **SRT8KXLI**

8.4 Additional Consideration

Payment terms per project - 25% advance payment against non-conditional LG , 25% against delivery of Items, 40% after final commissioning & signoff -10% retention until end of the warranty period.

8.5 Levels of Service

The Supplier's goal must be to meet, and even exceed, when possible, the levels of service described.

9 PREPARATION OF BID

9.1 Language of Bid

The Bid prepared by the Bidder, as well as all correspondence, documents relating to the Bid exchanged by the Bidder and ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E, supporting documents, and printed literature shall be written in English.

9.2 Documents Comprising the Bid

Each bid shall be in two parts: -

A. Part I- Technical Proposal.
B. Part II- Price Proposal.

The two parts should be in two separate covers, each super-scribed with the name of the Project as well as "Technical Proposal" and "Price Proposal" as the case may be.

Most provide the technical proposal in hardcopy and softcopy

The Supplier cannot quote for the project in part.

9.2.1 PART I - TECHNICAL PROPOSAL.

The technical proposal should reflect the ability of service supplier and must include the following:

1- Company profile with previous implemented project.
2- The vendor must be partner of delivered device model and certified.
3- The delivered solution including OS and software must pass the vulnerability security scanner and hardening based on CIS standard.
4- A project plane must be provided for implementation.
5- Solution design and architecture to be deliver and approve by ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E before project start up.
6- Deliver project documentation samples from previous project to ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E as guidance before starting project implementation.
7- A project documentation must be delivered after project completed.
8- The project is a turnkey solution.
9- CV for project implementers to be included and be reviewed by ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E team before project implementation start up and ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E have the right to reject anyone.
10- Delivery and acceptance criteria for each implemented point in the project will be reviewed by ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E before start implementation.

9.2.2 PART I I - PRICE PROPOSAL.

1- Company Financial Documents
2- All prices should be itemized and item price to include all related cost
3- All prices are in Egyptian pound or USD
4- Payment for USD offers will be in EGP according to central bank charges in time of payment
5- Price must include VAT and customs fees
6- 2024 company's budget

9.3 Submission of Bids

1- **Sealing and Marking of Bids:** The Bidders shall seal the envelopes containing "Technical Bid" and "Price Bid" separately and the two envelopes shall be enclosed and sealed in an outer envelope. The Bidder should additionally submit soft copies of the Technical Specification in the form of CD.
2- **Deadline for Submission of Bids:** Bids must be received by ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E at the address specified, no later than the date and time specified in the Invitation to Bid.

3- ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E may, at its discretion, extend this deadline for the submission of Bids by amending the Bid Documents, in which case, all rights and obligations of ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E and bidders, previously subject to the deadline, will thereafter be subject to the deadline as extended.

4- **Clarification of Bids:** During evaluation of the Bids, ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E, at its discretion, may ask the bidder for clarification of its Bid. The request for clarification and the response shall be in writing, and no change in the prices or substance of the Bid shall be sought, offered, or permitted.

10 TERMS AND CONDITIONS

10.1 Assignment

The Supplier shall not assign, in whole or in part, its obligations to perform under the Contract, except with the ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E's prior written consent.

10.2 Bidders:

The qualified bidder for this tender and his sub contactors must be Partner in the scope of requested equipment.

10.3 Quantities

Material quantities as specified are approximate and no guarantee is implied that the exact amount will be purchased.

10.4 Response and Resolution

The response and resolution time is mentioned for each service project in scope section.

10.5 Prices:

a) All prices must be in Egyptian pounds or USD and valid for 120 days after closing date of tender. However, for offers in USD, payment will be in EGP according to CBE rates at the date of payment.
b) The item prices are deemed to include all costs, freight, and other expenses (including customs and VAT) incurred by Supplier in delivering the goods to the location to Cornish Maadi Cairo Egypt as specified and performing his obligations under this Agreement.
c) The prices are fixed and shall not be subject to any variation. The supplier shall absorb the parts and labor of any missing components, if any, required to connect the items purchased by Alexandria International Containers Terminals S.A.E under this Agreement.

10.6 Risk, Loss, or Damage

ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E, unless stated the otherwise, shall not be responsible for any risk, loss or damage caused by events beyond ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E's control, including but not limited to the goods which are in the course of delivery to ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E, whether by land, sea or air, that will include any governmental or customs regulations.

10.7 Delivery Time

The SUPPLIER shall deliver the goods to ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E in accordance with the project schedule. In the event that SUPPLIER fails to deliver the goods on time, ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E shall have the right to cancel the order and/or claim any other form of relief or damages from supplier.

10.8 Acceptance by ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS

All deliveries of goods shall be subject to inspection and shall not be deemed to have been accepted until ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E furnished SUPPLIER with a formal acceptance notice. The signing of the Delivery Note by ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E is not deemed to be acceptance.

10.9 Warranty:

SUPPLIER warrants that goods delivered shall be free from defects in materials and workmanship. SUPPLIER undertakes to replace any defective parts and components and make good all defects in the goods swiftly and bears all costs including transport charges for replacing and repairing the defective goods.

10.10 Payment

Each Project will have its own Payment terms.

ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E shall assess a penalty on deliveries, which are not made in accordance with the project schedule; Penalty shall be in the amount of 1% percent of the section purchase price per week up to a maximum penalty of 10% of the purchase price.

10.11 Contract Terms and Conditions

ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E shall provide the supplier with all necessary documents to facilitate issuance of annual permanent gate permits for the supplier's technical support team and to be able to access sites at any time, in the event that the supplier was unable to issue a yearly permit.

The supplier has the responsibility of in/out transport of the spare parts needed inside the ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E locations as ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E will help the supplier to get their custody book.

The supplier shall not alter, modify, or change any configuration on any hardware/software without a written permission from ALEXANDRIA INTERNATIONAL CONTAINERS TERMINALS S.A.E.

11 DISCLAIMER

The information contained in this Request for Quotation (RFQ) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Alexandria International Containers Terminals S.A.E, is provided to the bidder(s) on the terms and conditions set out in this RFQ document and all other terms and conditions subject to which such information is provided.

This RFQ is neither an agreement nor an offer and is only an invitation by Alexandria International Containers Terminals S.A.E to the interested parties for submission of bids. The purpose of this RFQ is to provide the bidder(s) with information to assist the formulation of their proposals. This RFQ does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability, and completeness of the information in this RFQ and where necessary obtain independent advice. Alexandria International Containers Terminals S.A.E makes no representation or warranty and shall incur no liability under any law, statute, rules, or regulations as to the accuracy, reliability or completeness of this RFQ. Alexandria International Containers Terminals S.A.E may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFQ.