Stock Holding Corporation of India Limited
All India Integrated Financial Services

REQUEST FOR PROPOSAL FOR
MANAGED SECURITY SERVICES FOR SECURITY OPERATION CENTRE

Stock Holding Corporation of India Limited
(StockHolding)

RFP Reference Number: IT-04/2020-21
Date: 14-DEC-2020

Request for Proposal (RFP)
For
Managed Security Services for Security Operation Centre

REQUEST FOR PROPOSAL FOR
MANAGED SECURITY SERVICES FOR SECURITY OPERATION CENTRE

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or information provided subsequently to System Integrator(s) or applicants whether verbally or in documentary form by or on behalf of Stock Holding Corporation of India Limited *(StockHolding)*, is provided to the System Integrator(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by *StockHolding* to any parties other than the applicants who are qualified to submit the bids (“System Integrators”). The purpose of this RFP is to provide the System Integrator(s) within formation to assist the formulation of their proposals. This RFP does not claim to contain all the information each System Integrator may require. Each System Integrator should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. *StockHolding* 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 RFP. *StockHolding* may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

REQUEST FOR PROPOSAL FOR
MANAGED SECURITY SERVICES FOR SECURITY OPERATION CENTRE

RFP Document Details

Name of Organisation	Stock Holding Corporation of India Limited
RFP Reference No.	**IT-04/2020-21**
Requirement	Managed Security Services for Security Operation Centre
Interest free Earnest Money Deposit (EMD)	Rs. 2,000,00/- (Indian Rupees Two Lakh Only) by way of RTGS/NEFT to be paid to Stock Holding Corporation of India Limited as Earnest Money Deposit should be submitted separately before submission of online bids by way of RTGS/NEFT on/or before 27-DEC-2020 StockHolding's Bank Account No.: 004103000033442 Bank: IDBI Bank (Nariman Point Branch) IFSC: IBKL0000004 System Integrators with MSME certificate are exempted for providing EMD
Date of issue of RFP document	14-DEC-2020
Pre-bid online meeting	18-DEC-2020 , 11:00 A.M. onwards Details will be shared on StockHolding portal (https://corporate.stockholding.com/notices.html)
Date of Submission of online technical bids	From 27-DEC-2020 23:30 hrs. IST.
E-bidding to be facilitated by	M/s e-Procurement Technologies Ltd.(ETL), Ahmedabad, on behalf of Stock Holding Corporation of India Limited
Address for online submission of bids	Bid must be submitted online on **https://stockholding.auctiontiger.net**
Date for online Technical bid opening	28-DEC-2020 or onwards
Date of Technical presentation	FROM 31-DEC-2020 to 04-JAN-2020
Email Address	PRIT@stockholding.com
Date for Commercial Price bids submission	06-JAN-2021
Date for intimation of Qualification status	07-JAN-2021
Date for online commercial bid opening	08-JAN-2021
Contact Details of M/s e-Procurement Technologies Ltd.(ETL), Ahmedabad	Primary contact number 9081000427,9904407997 Imtiyaz Tajani: - 079-68136831, imtiyaz@eptl.in Salina Motani: - 079-68136843, salina.motani@eptl.in Jainam Belani: - 079-68136820, Jainam@eptl.in Ekta Maharaj: - 079-68136840, ekta.m@eptl.in Deepak Narekar: - 079-68136863, deepak@eptl.in Sujith Nair:- 079-68136857, sujith@eptl.in Devang Patel:- 079-68136859, devang@eptl.in
This bid document is not transferable	

Executive summary of the project

Stock Holding Corporation of India Limited is looking for the suitable system integrator (SI) to provide managed security service (MSS) / Security Operation Centre (SoC) Operations management from Stockholding's Data centre location. SI needs to provide a support for Managed, Detection and Response capabilities services procured by Stockholding and comply with the Service level agreements (SLA's) for all the in-scope devices under SOC Operations. Stockholding expects system integrator to have a proven experience in the implementation, integration and managing of Security Operation Centre (SoC).

The System Integrator shall understand StockHolding's overall Information Technology Infrastructure w.r.t. network and network-security architecture and device management of security solutions/ Services mentioned in this RFP and submit a response, to operate a 24*7 security operation center integrated with Stockholding IT Systems, Servers, applications, network and network-security appliances and devices using standard methods / protocols/ message formats to support Stockholding's critical applications.

The objective of this RFP is SOC Operations Management, Support for MDR Services integrations and management and also to comply with the circulars and advisories issued by, CERT-in, NCIIPC, SEBI, NSDL, CDSL, PFRDA, IRDA, RBI etc. and to implement a robust Security Operation Center (SOC) in Stockholding to prohibit/fight against Cyber Security Threats. The threat landscape will consist of the applications, servers, network appliance and other technologies that support the critical infrastructure.

Managed Detection and response (MDR) services at StockHolding is covered in the below functional principles:

- Detection of Information Security Threat & Prevention of Impact/ Breach: The MDR services are able to identify information security threats/ vectors targeting StockHolding's environment and prevent impact or breach due to them through implementation of adequate security mechanisms.

- Incident Management: Reporting and logging of information security incidents through the use of appropriate ticketing tools available in MDR Dashboard.. Track and monitor the closure of these information security incidents and Escalation of these incidents to appropriate teams/ individuals in the StockHolding.

- Continuous Improvement: Continuously improve MDR and SOC operations.

StockHolding is envisaging a Managed Security Services model under which the prospective system integrator shall provide 24x7x365 SOC Operations management and monitoring from StockHolding SOC. The scope would involve monitoring of core infrastructure and security components at StockHolding's Managed Data Centre at Mahape, StockHolding's Subsidiaries, Disaster Recovery (DR) Site at Bangalore, Head Office, Parel, Near DR (NDR) Site in Airoli, Fort branch office and any other offices in India.

The System Integrator is required to integrate the core IT Infrastructure Devices including Servers, Active Directory Setup including DNS, WINS, DHCP Server and respective services management across Stockholding and branch locations, Network Switches, routers, Firewalls/UTM, IPS appliances, Web Security

Appliances, Intrusion Prevention Systems, File Integrity Monitoring Solution, Data Leakage Prevention Solution, Web Application Firewalls, Privilege identity Management (PIM) Solution, Anti APT Solutions, Network Behavioral Anomaly Detection, Network Access Control, DAM, Data Leakage Protection (DLP), Data Classification of all IT Assets, Risk Assessment and Risk Treatment of all IT Assets, etc. with the MDR and Clean pipe solution. Logs received from all these devices has already been correlated but needs to be analyzed for detection of threats, unusual user behavior & proactive incident analysis in real time manner.

Eligibility Criteria

The System Integrator must possess the requisite experience, strength and capabilities in providing the services necessary to meet the requirements, as described in the tender document.
The System Integrator must also possess the technical know-how and the financial wherewithal that would be required to successfully manage the Security Operations Centre along with MDR capabilities.

The System Integrator should have the expertise to secure overall Information Technology setup of StockHolding comprises of Servers, Secure Active Directory and SCCM Deployments, Extranets networks, MPLS Network, Perimeter network architecture, Email setup, Site to Site, IPSec and SSL VPN deployments.

Security Operation Centre (SOC) team needs to perform a role of device management which includes and not limited to installation, implementation, configuration, reconfiguration, Backup and restoration management of the network-security appliances like firewalls, Intrusion prevention and detection appliances, Site to Site, IPSec and SSL based Virtual Private Network appliances, Web Application Firewalls, Privileged Identity Management devices, Load balancers, Security of Internet and WAN based routers and switches, Secure broadband connectivity, In house and / or Cloud based proxy along with URL filtering and management services, MDM Services, NTP Server and Services, Database activity monitoring, End to end antivirus management of clients and Servers and other network equipment as sought by StockHolding under managed services for DC at Mahape, DR at Bangalore, NDR at Airoli, Extranet setup.

The bids must be complete in all respect and should cover the entire scope of work as stipulated in the tender document. The invitation to bid is open to all System Integrators who qualify the eligibility criteria as given below. Eligibility criteria are mandatory and any deviation in the same will attract bid disqualification.

The following are the key qualification criteria:

#	Eligibility Criteria	Supporting Evidence
1.	The System Integrator should be in existence for minimum of 15 years as on 31-OCT-2020 and providing Cyber Security services for at least last 10 years.	Certificate of Incorporation

2.	The System Integrator should have the experience of owning and managing a well-established Security Operations Centre (SOC) for at least 10 years in India. System Integrator shall provide the details of the SOC including the location, infrastructure, tools used, companies served, process and methodology, staff employed.	Self-Declaration from equivalent to Company secretary with Supporting documents should be a SOC related PO dated 13-DEC-2020 or before
3.	The System Integrator should have executed, during any of the last five financial years, at least one SOC contract having value not less than INR 15 Crores OR two SOC contracts having value not less than INR 8 Crores each for any Govt./ BFSI/ PSU/Enterprise organization globally	Self-Declaration from equivalent to Company secretary.
4.	Annual Audited Turnover during last three financial years (as per the last published audited balance sheets) should not be less than INR 100 Crores. AND At least INR 35 Crores from InformationSecurity (IS)/ Managed Security Services(MSS) related services and products during any of the last 5 FYs. AND The current Net worth of the System Integrator should be positive.	Self-Declaration from equivalent to Company secretary. CA Certificate with CA's Registration Number/ Seal as per "Specific Requirements". It shall clearly state the'Overall Average Annual Turnover' and 'OverallAverage Annual Turnover from IS/ MSS'.
5.	System Integrator SOC should be ISO 27001 and /or ISO 20000 certified and SOC 2.0 accredited.	Certificates.
6.	The System Integrator should have in minimum 3 BFSI customers in India who are using SOC services from the System Integrator for at least last 5 years	Customer references to be provided
7.	System Integrator should be providing NGSOC services to 3 BFSI Customers using proposed SIEM solution which leverages Big Data analytical platform that is capable of detecting anomalies in the network over and above rule/ use case-based technologies can detect.	To provide 3 BFSI clients PO for Next Generation SOC Services

8.	The System Integrator's SOC service should be recognized by leading analyst's like Gartner in their market guide for last three years	Share analyst reports to confirm the same.
9.	The System Integrator must be empaneled with CERT-In as Information Security Audit Organization	Self-Declaration from equivalent to Company secretary
10.	System Integrator should have below mentioned best in class tools/technology & application listed in latest Gartner quadrants report which must be fulfilling the NHB business requirements:· SIEM· Threat Intelligent Feed	Self-Declaration from equivalent to Company secretary
11.	The System Integrator Company should have at-least 100 qualified Information Security / Cyber Security Professionals (DISA/CISA/CISSP/CISM/CDAC/ CEH/ITIL/PMP/ISO 27001/CCSA certified) in their payroll.	Self-Declaration from equivalent to Company secretary
12.	The system Integrator shall not assign or sub-contract the assignment or any part thereof to any other person/firm.	Self-Declaration from equivalent to Company secretary
13.	System Integrator SOC should be owned by them and not outsourced to any third party	Self-Declaration from equivalent to Company secretary

System Integrator should submit documentary evidence (acceptable to StockHolding) of the Information given in the related formats in respect of all above mentioned criteria while submitting the proposal. Proposal of System Integrator who do not fulfil the above criteria or who fail to submit documentary evidence to the satisfaction of StockHolding would be rejected.

Technical Bids will be evaluated for the following broad parameters and a score would be given to each System Integrator by StockHolding based on the scoring criteria mentioned below-

S.No	Evaluation Parameters / Credentials	Credentials for awarding Score (It should be clearly understood that in case of ambiguity or lack of clarity in the documents submitted, the decision of StockHolding is final for awarding the marks against each of the specified items.)	Maximum Marks
1	System Integrators no. of Years of experience in providing Managed Security Services(MSS) along with Security Operation Centre (SOC) services (As on 31st March 2020)	The marks to be awarded as per the credentials submitted in respect of clients serviced in India: 20 Marks for 15 years and above. 15 Marks for 12 years and above. 10 Marks for 10 years and above. Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.	20
2	The System Integrator's experience in providing Managed Security Services (MSS) along with Security Operation Centre (SOC) services in India to BFSI/PSUs in India. (As on 31st March 2020)	The marks to be awarded as per the credentials submitted in respect of BFSI/PSUs serviced: 20 Marks for 5 BFSI/PSUs or above. 15 Marks for 4 BFSI/PSUs. 10 Marks for 3 BFSI/PSUs. Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.	20

3	No. of BFSI/PSUs where the proposed SIEM solution should have been providing SOC services in India during the last three years (As on 31st March 2020)	The marks to be awarded as per the credentials submitted in respect of BFSI/PSUs serviced: 20 Marks for 5 BFSI/PSUs or above. 15 Marks for 4 BFSI/PSUs. 10 Marks for 3 BFSI/PSUs. Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.	20
4	The System Integrator's inclusion in the Gartner or Forrester reports on Managed Security Services (MSS) or Managed Detection &Response Services (MDR) specifically in past 3 years (2020, 2019 & 2018)	The marks to be awarded as per the credentials submitted in respect of no. of years: 20 marks for inclusion in both Gartner & Forrester. 15 marks for only 1 analyst recognition. 10 marks for only 1-year recognition. Please provide relative document of the Gartner or Forrester reports fulfilling the mentioned criteria.	20
5	System Integrator having a SoC and DR SOC functional in India for: (Max Marks 10)	More than 4 years -------------- Marks 10 4 years --------------------------- Marks 05	10
6	The System Integrator's SOC infrastructure must be ISO certified and must provide SOC -2 audit report.	(System Integrator must provide a copy of valid ISO Certification for the SOC facility and extract of most recent SOC-2 report) (Max Marks 10)	10

Current State of SOC

The Security Operations Centre is currently managing security device management based on a centralized model with onsite resources located at the Primary Data Centre at Mahape and may require to managed from DR at Bangalore if need arises during the contract period of 3 years.

StockHolding's Network has a hub-less or full mesh, Hub WAN architecture built by leveraging BSNL and TCLs' MPLS VPN services. StockHolding expects suggestions and recommendations for Secure Network Architecture (SNA) from proposed System Integrator as currently MPLS setup has been designed with BSNL and TCL service providers with a dual last mile connectivity (across ISPs) for the BSNL and TCL backhaul links, from StockHolding's head-end router/s located at the DC at Mahape & DR at Bangalore. The TCL MPLS VPN is also used for replication, Video Conferencing, and server related traffic apart from providing connectivity over last mile WIMAX to the branches.

StockHolding expects that proposed System Integrator will conduct SNA of entire network architecture and provide us a details report along with gap analysis and recommendation to bridge those gaps till the entire duration of contract period. All the regional and branch offices are currently connected to the BSNL MPLS network over single MPLS links, in future it is proposed to have dual last mile connectivity at the branches too. Few branches are connected to the regional offices/DC over P2P links, the existing backup is provided over WiMAX/ Broadband / ISDN / CDMA /RF connectivity etc. StockHolding also has SAN to SAN replication links.

The System Integrator will be required to design/re-design, configure/re-configure, monitor, maintain and secure present network security setup i.e. Firewall and IPS appliances, Internet proxy services, Suggestions and recommendations for Securing Active directory architecture deployment as per the need basis and provide the appropriate steps to be provided to Secure Active Directory deployment with DNS, WINS and DHCP Services and Domain management , Patch management with WSUS and or SCCM Server and Services, Secure NTP Server and services, End to end Antivirus management, Secure guidelines for Cisco ISE Appliances and Spam mail services with Cisco ESA Iron port appliances, Site to Site, IPSec and SSL based Virtual Private Network appliances, Web Application Firewalls, Privileged Identity Management devices, Load balancers, Securing WAN and Internet routers and switches, Securing broadband and Wi-Max connectivity, In house and / or Cloud based proxy along with URL filtering and management services, MDM Services NTP Server and Services, Database activity monitoring, Securing local break out connectivity, Internet links with DDoS Services, MPLS security, Securing WLAN controllers, Wireless APs, WLAN monitoring systems, load balancers, etc. of StockHolding which will include but not limited to co-ordination with ISP link providers, managed DDoS detection and mitigation services etc.

The System Integrator will responsible for the configuration management, Vulnerability assessment (On Half yearly basis) of Organizations Servers network-security equipment's i.e. Firewall appliances, IPS Appliances, Load balancers, Layer 2 and Layer 3 switches and routers, ISE Appliances, Internet routers, Iron port appliances and Securing Video Conferencing equipment, Securing WLAN controllers, Securing Wireless APs, Secured WLAN monitoring systems, load balancers and servers managed by StockHolding etc. under a managed service for DC, DR, Extranet DR, and assisting StockHolding in securing StockHolding's network security architecture by coordinating with the concerned service providers.

Detailed Scope of Work

The scope of work to be undertaken by the System Integrator shall be for MANAGED SECURITY SERVICES TO RUN SECURITY OPERATION CENTRE (SOC) SERVICES along with services and support for MANAGED, DETECTION AND RESPONSE (MDR) services procured by StockHolding.

StockHolding is looking for a Security Service Player who shall provide a "second layer of eyes approach" on the existing internal Security Controls & Monitoring services & help in augmenting the existing internal capabilities by having advanced SOC capabilities focused on detection of advanced threats apart from the traditional rule based SIEM capabilities such as-: MDR Methodology (Managed Detection & Response), which can help StockHolding to have a proactive approach in determining the known & unknown threats faced by StockHolding to reduce the risk of breach of data & systems, the advanced features/capabilities expected out of the System Integrator apart from rule based monitoring such as employing off the shelf SIEM solutions are as follows

Number of Active Models to be analyzed as same has been monitor and included under Managed Detection and Response Services and necessary actions to be initiated by coordinating with respective StockHolding Team members. Upon Confirmation from respective team MDR case needs to be close in MDR Dashboard as per Service Level agreement.

- Security Analytics , Monitoring& Feeds services.
- Threat Hunting.
- Incident Analysis & Response.
- Detect Unknown attacks, blind spots & deep detection.
- Augmentation of rule-based detection systems with new approaches such as machine learning & Artificial Intelligence to detect patterns, abnormalities.
- Anti-Phishing and Brand Monitoring.
- Forensic as a SERVICE - forensic , log and advance malware analysis/ Forensic and Log Analysis.
- Attack Detection Network
- Attack Detection Application
- Data Exfiltration.
- Dynamic DNS.
- Firewall Volumetric Anomaly – Connection.
- Firewall Volumetric Anomaly – Packet Transfer.
- Lateral Movement – Malicious process.
- Lateral Bot.

- Malware Beaconing.
- Process Anomaly.
- Watering Hole Attack

Device Management

Development and implementation of processes for management and operation of the SOC including (but not limited to) the following devices and processes.

The System Integrator should support and integrate data (log and/or flow) collection from different OS and their versions but not limited to Windows, Linux, AIX, Solaris etc., networking devices, security devices and solutions, physical access control systems, etc., as required by StockHolding.

- Secure Active Directory Deployment across Stockholding and branch locations including DNS, WINS, DHCP Services etc. on premises and on cloud.
- In scope devices, servers, appliances planning and design;
- In scope devices, servers, appliances services Implementation;
- In scope devices, servers, appliances performance and capacity management;
- In scope devices, servers, appliances fault management.
- In scope devices, servers, appliances Incident Management.
- In scope devices, servers, appliances Change Management.
- In scope devices, servers, appliances fault management.
- Vendor Co-ordination and Escalation Management.
- Configuration Audit (CA) of Servers, Network devices, Security appliances, Layer 2 and Layer 3 Switches and routers.
- Vulnerability Assessment (VA) of Servers, Network devices, Security appliances, Layer 2 and Layer 3 Switches and routers.
- Internal and external Penetration Testing of Servers, Network devices, Security appliances, Layer 2 and Layer 3 Switches and routers.
- Log Monitoring and Log analysis within MDR platform and coordinating with respective team for closure.
- System Integrator to on board / integrate IT Assets of StockHolding devices. Correct log baseline & configuration changes required for effective correlation & monitoring.
- Red Team Assessment.
- Remote Exposure and Breach Assessment.
- Cyber Security Drill.
- Secure Network Architecture (SNA) along with Risk Assessment and Risk Treatment (RA/RT) Methodology.

- Support for In-scope application specific databases like SQL etc. from System Integrator’s backend team for Database management, Log synchronisation with DC-DR communication and policies to be establish for backup and restoration.
- Internal Nessus Scan management for scanning internal servers as on need basis and reports to be provided as per the requirements.
- Device management team should provide support as per the ISMS policies and procedures of StockHolding as should adhere to the changes as per the modifications in ISMS policies and procedures of Information Security and Cyber Security from time to time.
- Data Classification, Risk Assessments and Risk Treatment of all IT Assets with the EDR and MDR and Clean Pipe solutions
- Work from Home Security.

The scope of services relevant to Network-security device management services includes the following:

- Secure Active Directory Deployment across Stockholding and branch locations including DNS, WINS, and DHCP Services etc. on premises and on cloud.

- The selected System Integrator will manage and monitor all the In-scope network-security devices from the SOC situated at StockHolding’s primary data centre at Mahape and manage the in scope network security devices placed in Near DR at Airoli , Centre point, Fort location and DR Site at Bangalore.

- The selected System Integrator is required to prepare/modify the network-security architecture diagrams for primary Data Centre (DC) at Mahape, Disaster Recovery (DR) at Bangalore, Extranet DR as per the requirement of StockHolding and the same will be submitted to StockHolding team on quarterly basis for review.

- The System Integrator is required to modify/redesign the existing Network-Security architecture (functionality and security) wherever required. In case of such requirements, System Integrator will provide detailed documentation on the modifications to be made thereof to StockHolding team for final approval. The System Integrator is also required to conduct POC/s for the network-security infrastructure related equipment/software’s/appliances/services/solutions etc. as and when requested by StockHolding team.

- The selected System Integrator will ensure appropriate Network-security Infrastructure architecture (functionality and security) is put in place, and conduct methodical reviews/assessments on a yearly basis (to identify any gaps/loopholes OR areas for concern OR Improvement/optimize the required functionality and security in the existing network-security architecture design) and mitigate the same, with particular emphasis to existing compliance requirements (ISO27001:2013, RBI, SEBI, PFRDA,IRDA, NSDL, CDSL etc.) along with thorough documentation.

- The selected System Integrator is required to provide all assistance to StockHolding officials for successfully conducting the DR Drills & BCP (Business Continuity Planning) Drills as per StockHolding's IT & BCP policy.

- The System Integrator has to liaison with the internet service providers in case of any issues in the internet links at DC at Mahape & DR at Bangalore and complete the necessary analysis for DDoS setup related findings and queries put across by Internet service provider.

- Asset Management and movement of all the in-scope devices of network and network-security within StockHolding's DC at Mahape & DR at Bangalore, Centre point and Fort location branches in Mumbai.

- The selected System Integrator will do the complete management and monitoring of firewall suite consisting of Checkpoint firewall appliances with Checkpoint software, Web Application firewalls, Cisco firepower FPD and FMC firewall appliances, ISS IPS appliances with Site Protector software, URL Filtering Tool, Squid Proxy Server, Management of VPN through Secure remote and secure client, Site to Site VPN, SSL Array VPN appliances, Trend Micro antivirus setup along with end point management, Syslog Server, NTP Servers, WSUS and SCCM Server for patch management, ISPs Setup, Application Load balancers, Application load balancer switches. Cisco ISE appliances, MDR Log Management and correlation, Cisco Iron port appliance management and maintenance, Securing Wi-Fi Controllers and Wi-Fi APs and other allied security products.

- Trend Micro Endpoint Detection and Protection :

  Antivirus Servers and Clients Management along with control mechanism: Trend-Micro Anti-Virus Suite - Inclusive of Installations / reinstallations, configurations & regular maintenance on all Servers and clients. Keeping Up to-date antivirus version, pattern file update, Virus scan engine, Spyware scan and pattern file engine on all servers and clients. Coordination with branches for antivirus scan engine, pattern file updates and patch updates.
  Major Tasks Include:

  - Advanced Malware and Ransomware protection. : Protects end points, on or off the StockHolding network against malware, Trojans, worms, spyware, ransomware and adapts to protects against new unknown variants as they emerge.

  As StockHolding has procured additional features for endpoint detection and protection, we expect on Site SOC team to do necessary analysis on following features and close within the SLA parameters. SOC team has to coordinate with respective end user and close the issue and report the same to designated StockHolding officials from time to time basis and record the same in monthly managed Information Security report.
  Features include:

- Context-aware EDR, recording, and reporting of system-level activities to rapidly assess attacks.
- Detailed root cause analysis (RCA) shows source and spread of attacks.
- Threat hunting tools leveraging Indicators of Attack (IOA) and behavioural analysis rules.
- Detects and analyses advanced threat indicators such as file less attacks.
- Complete visibility – Helps understand full impact of detections, including how many users were compromised or which user was 'patient zero'
- Endpoint sweeping – Perform searches (Sweeping) for indicators of attack, such as malware, registry activity, running processes and more. Open IOC or YARA files can be used to as search criteria as well
- Advanced threat hunting – Investigators can perform threat hunting based on indicators of attack (IOAs). This allows investigators to develop attack discovery rules or work with the IOAs provided by Trend Micro to hunt for threats
- Rapidly responds before sensitive data is lost.
- iDLP, Application Control and Virtual patching.
- Server protect for Windows, Linux Servers.
- Deep Security for AIX Servers.

SLA for Endpoint detection and Protection

- Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.

- SOC team should have implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information to external parties.

- The response and recovery plan of the SOC team should have plans for the timely restoration of systems affected by incidents of cyber- attacks or breaches

- Any incident of loss or destruction of data or systems should be thoroughly analysed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

- To ensure that all the network infrastructure devices and servers are protected from intrusions and have proper tools and mechanisms to monitor and protect from intrusions.

- Regular reporting on health, performance of network security devices and assets deployed.

- End to end Patch Management on all the aligned Servers connected to StockHolding network and in-scope network-security servers, appliances and devices.

- Migration of IPv4 to IPv6 (As and when required)
- The System Integrator should Monitor and manage all the in scope network-security devices (Appliances, servers, routers, switches) and Internet links for strict compliance with SLA.
- Liaison with Internet Service Provider.
- Internet Bandwidth Optimisation by defining quality of service on perimeter firewall as well as on perimeter routers.
- Ensure availability and optimum utilization of all network-security components, servers and devices.
- Documented processes, procedures, suggestions and recommendations for securing Wireless Network Security.
- Vulnerability Assessment and Configuration Audit along with confirmatory reviews on half yearly basis for all the servers, network devices includes switches, routers, network-security devices belongs to StockHolding IT Assets.
- Penetration Testing along with confirmatory reviews for all the servers, network devices includes switches, routers, network-security devices belongs to StockHolding's IT Assets.
- Comprehensive Documentation.
- Rule base Reviews : Firewall, IPS, Load balancers, ISE Appliances, Iron port appliances, Wi-Fi Controllers and access points, DMZ Switches, L3 Switches and Router Configuration and rule base reviews (Internal and perimeter level) as per calendar activities prepared by Networking.
- Risk Assessment of network-security devices on yearly basis and reporting with proper analysis with industry supported guidelines.

Network and network-security devices and Servers under device management :
Network Security devices and Servers to be monitored under device and configuration management include but are not limited to the following:

Devices		Mahape	Bangalore	Fort
Routers (Internet Routers)		05	02	00
Switches	Cisco L2 Switches	18	18	00
	Load Balancers	06	02	00

In Scope Servers – Windows		11	06	00
In Scope Servers – Linux		10	03	00
Firewall Appliances	Checkpoint	05	05	00
	Cisco FMC	01	01	00
	Cisco FPD	04	02	02
Cisco ISE Appliances		01	01	00
IPS Appliances		04	02	00
Wi-Fi Controllers		02	00	00
Iron Port Appliances		01	01	00
Imperva WAF		02	01	00
Array VPN Appliances.		02	02	00
Total Number of devices		72	46	02

High Level Deliverables

Areas	Activities	Deliverables
Security Monitoring	Log Monitoring; Server Monitoring; Security and Network Device monitoring	• 24*7*365 log monitoring • Detection of threats from integrated log sources and based on the use cases defined. • Event Analysis • Alerts as per defined escalation matrix
Network Threat Hunting	Analytics Based Hunting & IOC Based Hunting	• Ongoing continuous process. • Notification of alerts generated through analytical models on Threat Hunting enabling hunting for attacks including but not limited to Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, Dynamic DNS attacks etc.
Incident Management	Incident Analysis, Identification of all components of the incident, root cause analysis and mitigation plans	• Provide logs and incident report for any identified security incident. • Coordinate with StockHolding's team and help to contain attack/incident. • Provide evidences for legal and

		regulatory purpose in the form of log data.
SOC Maturity Improvement		• Quarterly briefings on Analysis and insights from data: trends, high risks areas, roadmap for strategic improvements, security posture benchmarking. Briefings on global threat trends, regulatory trends and cyber technology trends.
Report Management	Periodic reports; Trend analysis; Customized reports	Review multiple reports including top attackers, attacks, attack targets, trends. • Monthly MIS reports for monitored devices. • Recommendation for improvement of security posture and threat landscape.
Global Intelligence Feeds(Optional)	Continuous and regular global feeds from external known agencies.	• Threat & Vulnerability advisories in form of E-mails. • Recommendations for security improvements. • Provide Historical, Operational, Analytical and predictive Analysis.

SOC Operations

The Selected System Integrator will develop the work flow process for attending to the various functions at the SOC including the work flow for attending to the incidents generated with network-security device management. System Integrator will develop documents such as Standard Operating procedures for smooth functioning of SOC.

System Integrator will provide support to already established full featured MDR service along with Incident Management capabilities. In future System Integrator will configure and integrate DAM, PIM, any other new security device, and Cloud based services in consultation with StockHolding and MDR team to generate meaning full incidents/reports and reduce the generation of false positives and operate the SOC Operations. System Integrator will manage SOC operations in consultation with StockHolding's team.

StockHolding has the right to use the MDR services of tool for the functions provided by the tool from StockHolding branches, subsidiary units, joint ventures, geographical location of the devices being monitored. StockHolding will also have a right to use the services of the tools from different locations. System Integrator has to keep a note of the same and integrate the devices from centralized location.

Intended Principles of the Managed Detection and Response (MDR) Service:

The principles that form the underlying platform for the MDR Services under Managed Detection and response are as follows. The services offered should follow from these principles. The "System Integrator" is expected to adhere to these principles while supporting this service.

Functional Principles:
The intent for SOC device management / Managed Detection and response Solution service is covered in the below functional principles:

- Device Management, Prevention & Identification of Information Security Vulnerabilities: The SOC device management solution and SIEM Service operations should be able to identify information security vulnerabilities in StockHolding's environment and prevent these vulnerabilities.

- Incident Management: Reporting of information security incidents through the use of appropriate tool centrally managed dashboard to track and monitor the closure of these information security incidents and escalation of these incidents to appropriate teams/ individuals in StockHolding.

- Continuous Improvement: Continuously improve SOC device management / Services / Solutions.

Scalability Principles:
The services/ solutions offered are modular, scalable, and are able to address StockHolding's equipment during the period of contract.

Availability Principles:
The services/ solutions in scope designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime as outlined in this RFP.

Performance Principles:
The services/ solutions offered should not have any significant impact on the existing Infrastructure/business of StockHolding either during integration or during operation of SOC.

Based on the above principles, the following services/ solutions have been identified to enhance the security posture of StockHolding:

- Security Information and Event Management (SIEM)
- Security Intelligence Services.
- Security Advisory Services.
- Anti-Malware Services.

The System Integrators who wish to take up the project shall be responsible for managing the MDR Services procured by StockHolding for devices managed under Data Centre (DC) at Mahape and Disaster Recovery Site (DRS) at Bangalore.

- Integration of new devices (Servers, Applications, Databases, network devices, security devices under the respective services/ solutions including configuration, customization as per the requirement of StockHolding.
- MDR tool has provided a comprehensive single dashboard view of the security risks/ incidents for StockHolding.
- Work/ Liaison with the MDR team System Integrator(s) and various application vendors of StockHolding for integration of services/ solutions of existing / New application platforms, servers, security devices, storage environments, enterprise network, and security solutions, etc.
- Development of operating procedures in adherence with StockHolding's policies.
- Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to designated team and official of StockHolding.
- Continual improvement of the Security Operations Services as defined in the SLA.

Support for Managed Detection and Response Services (MDR Services):

The MDR solution/ service are collecting logs from security and network devices, appliances, servers and various application and database server security logs. The System Integrator is expected to perform thorough log analysis and take necessary action for In-scope devices as well as co-ordinate with respective internal team members of StockHolding and close the MDR tickets generated in dashboard to ensure compliance.

- **Log Collection**

  Logs from all the in-scope and other StockHolding Servers and network devices located at the geographically dispersed location should be collected. System Integrator should coordinate with MDR team and follow the baseline document provided by MDR team and provide the necessary inputs to StockHolding team for the level of logs to be enabled from different components of IT infrastructure assets. The log baseline should be in line with global best practices. In case the systems/applications are writing logs to the local hard disks, System Integrator is expected to provide solution to pull the logs from these devices through secure transfer. Only in case where remote log collection is not feasible, System Integrator should install agent on respective servers and applications for collection of logs by coordinating with respective support team members of StockHolding. Raw logs should be made available in case of legal requirement for number of years of compliance requirement followed by StockHolding.

- **Logging of critical devices**

- The System Integrator is required to maintain the syslog of critical network devices installed at DC, DRC and Critical locations for a period of three months. The logs should be onsite for three months thereafter logs can be stored on tapes and submitted to StockHolding.
- The System Integrator has to ensure that the logs from Critical network devices are being stored in the syslog servers on regular basis.
- The periodicity for the retention of the log will be reviewed by StockHolding officials on quarterly, half yearly and yearly basis and same has to be ensure by System Integrator.
- System Integrator will design and implement all simple scripts that may be needed to analyse logs and produce reports as required by StockHolding officials.

- **Log Aggregation and Normalization**

  Logs collected from all the devices should be aggregated as per the user configured parameters. Logs from multiple disparate sources should be normalized in a common format for event analysis and correlation.
- **Log Encryption, Compression and Transmission**

  Collected logs should be encrypted and compressed before the transmission to the remote Log Correlation Engine.

- **Log Archival**

  Logs collected from all the devices should be stored in a non-tamper able format on the archival device in the compressed form. Collection of Logs and storage should comply with the Regulatory requirement and should maintain a chain of custody to provide the same in the court of law, in case the need arises. For correlation and report generation purpose, past -3- months log data should be available online. Logs prior to -3- month's period should be stored on removable media.

  System Integrator will ensure that retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols.

- **Log Correlation**

  Currently collected Logs are correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules are predefined and also user configurable. System Integrator will coordinate with MDR team and ensure that correlation rules should be customized by them on regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection of any such incident, coordinate with MDR team and correlation rules must be customized immediately to capture such incidents.

- **Alert Generation**

Current MDR Solution is capable to generate alerts, register and send the same through message formats like SMTP, SMS Syslog, SNMP, and XML as per user configurable parameters. System Integrator has to ensure that all such alert mechanisms are intact and brought to the notice of StockHoling team during their tenure on immediate basis to ensure compliance.

- **Event Viewer/Dashboard/Reports/Incident Management**

MDR Solution is capable and providing web based facility to view security events and security posture of StockHolding's Network and register incidents. System Integrator's onsite team should analyze the logs on regular basis and drill down MDR's capability to view deep inside the attack and analyze the attack pattern. Dash board have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc. MDR Solution is providing various reports based on user configurable parameters and standard compliance reports for ISO27001:2013 and regulatory reports. System Integrator has to ensure that StockHolding should get all the configured reports to ensure compliance.

Selected System Integrator will customize incident management/dashboard/reports by coordinating with MDR team and provide meaningful reports to StockHolding and will modify the same as per the changing requirement of StockHolding.

- **Integration with in-scope monitored devices**

System Integrator's onsite team members should have expertise on MDR and SIEM solution and should suggest the detailed commands/guidelines for integration of the other in-scope devices with the SIEM to be integrated in future. System Integrator will be required to integrate all the devices supplied as part of this RFP.

- **Development of Connectors for customized applications/ devices.**

While it is expected that connectors for all the standard applications and devices will be readily available in the collector and Log management devices, connector for mostly in-house/custom built applications will need to be developed. As MDR team deployed for SOC operations will be expected to develop applications connector, in house SOC team of System Integrator expected to support them for integration of devices as per the custom connectors provided to them by MDR team.

- **Workflow Automation.**

Selected System Integrator will define the work flow automation so that applications are integrated and manual intervention is minimal.

- **Integration of devices in Managed detection and response along with SIEM Services:**

- ✓ Integrate the devices with MDR and SIEM to collect logs from the identified devices, applications, and databases etc.
- ✓ Develop parsing rules for non-standard logs.
- ✓ Implement correlation rules of the SIEM solution/ service design and provided by MDR team.
- ✓ 24X7X365 log monitoring for in scope devices and applications.
- ✓ Rapid real-time response to incidents.
- ✓ Evaluation of incidents.
- ✓ Forensics to identify the origin of threats, mitigation thereof, initiation of measures to prevent recurrence.
- ✓ The SIEM solution/ service shall also have capability such that StockHolding Team can also execute the queries to identify custom made scenarios/incidents.

- **MDR Sizing**
  The expected EPS count for StockHolding should be a minimum of 2,000 and scalable to 4,000. The System Integrator needs to coordinate with MDR team and provide support for MDR services that cater to as per the requirement of devices on boarded with MDR.

Annexure - A

- IT Assets of StockHolding included and to be included and monitor in MDR Solution should include but are not limited to the following

- Network, Security Devices and Servers to be considered for Configuration Management, Vulnerability Assessment and Penetration Testing (Internal and External), Secure Network Architecture and Risk Assessment and Risk Treatment Activities are as shown below.

Serial Number	ACTIVITY	SCOPE	FREQUENCY	MODE
1	Network Penetration Testing	Internal - Up to 180 IP Addresses	Twice a Year (2 Initial test + 2 Confirmatory test)	On-site.
2	Wireless Penetration Testing with 5 SSID's per location	Number of locations: (Navi Mumbai and Mumbai)	Twice a Year (2 Initial test + 2 Confirmatory test)	On-site.
3	Firewall rule base review – Will be performed by device Management team.	Checkpoint – 2; Cisco FPD – 8 and FMC – 2	Twice a Year (Initial + Confirmatory)	On-site
4	Red Team Assessment	Internet facing Assets	Once a Year (Initial +Confirmatory)	Off-site
5	Cyber Security Drill	IT Assets	Once a Year (Initial +Confirmatory)	On-site / Off-site

6	Remote Exposure and Breach Assessment		Once a Year (Initial +Confirmatory)	On-site / Off-site
7	SOP Review	In-Scope Devices	Once a Year (Initial +Confirmatory)	On-site
8	Router ACL Review – Will be performed by device Management team	10	Once a Year (Initial +Confirmatory)	On-site
9	Configuration Audit (CA), Vulnerability Assessments (VA) & Penetration Testing (PT) - (As per CIS Benchmark and close the gap's and provide the clean report)	180	Twice a Year (2 Initial test + 2 Confirmatory test)	On-site / Off-site
10	Wi-Fi Controller Rule base review	2	Once a Year (Initial +Confirmatory)	On-site
11	IPS Review – Will be performed by device Management team	6	Once a Year (Initial +Confirmatory)	On-site
12.	AdHoc network security assessment	Up to 5 IP Addresses / 5 Apps in a year PT: 5 IP's Black / Grey Box Scan – app – 5 apps	Twice a Year (2 Initial test + 2 Confirmatory test)	On-site
13	Vulnerability Assessment and External PT (With White listing and Without White listing)	50IP Addresses + Additional 10	Twice a Year (2 Initial test + 2 Confirmatory test)	On-site
14	Internal Nessus Scan.	1200 IP Addresses	As on need basis.	On-site
15	Backup and Restoration.	In-Scope Devices	Yearly Once	On-site
16	Network and Network-Security devices Failover Testing.	In-Scope Devices	Twice a Year	On-site
17	Adhoc Revalidation post any planned / unplanned audits findings implementation	Up to 10 Units PT	Initial Test + Confirmatory	On-site
18	Report Analysis	VA PT Audits	Quarterly / Half yearly	Onsite

Other Activities	
Review of MDR Tickets Alerts and Closure	Daily
updated System and Offline Systems AV Report	Daily

Advisory Actionable attracting Configuration Changes on Cisco Router	Daily
URL hit count report	Daily
mDDoS Report Analysis	Daily
Proxy Failover Testing	Weekly
USB Access Review	Quarterly
User-id Recertification	Quarterly
Data-Centre Password Register	Quarterly
IOS, Firmware/Application Up gradation	Quarterly
Network Diagrams Updates	Quarterly

Note: These activities may modify along with their frequency during the course of contract period as per the compliance requirement. Stockholding may add additional calendar activities as per addition of new device / Applications (In house or Cloud based) in SOC Operations Management during period of 3 years.

Annexure -B

SL NO	ACTIVITY	SCOPE	DELIVERABLE	FREQUENCY	LOCATION
1	Network-security Infrastructure architecture (functionality and security) is put in place, and conduct methodical reviews/assessments on a yearly basis (to identify any gaps/loopholes OR areas of concern and Improvement.	180 IP Addresses	SNA Report	Onsite & Yearly	Navi Mumbai
2	Risk Assessment of network-security devices on yearly basis and reporting with proper analysis with industry supported guidelines.	180 IP Addresses	Risk Assessment Report	Onsite & Yearly	Navi Mumbai
3	Ensuring adequate, appropriateness and concurrency of various policies and guidelines in place and shall provide Information Security consultancy for newer	15 Policies & Procedures to be reviewed & 5 new policies and procedures Development.	15 Policies & Procedures to be reviewed & 5 new Policies Development	Onsite & Yearly.	Navi Mumbai

	technology deployment for new and existing applications and products.				
				Offsite & Yearly	Navi Mumbai
4	Assisting StockHolding in planning, execution, and implementation of information security related initiatives/projects/programs in StockHolding.	Handholding & Assistance to StockHolding in implementing Information Security	Advisory Support	Offsite & Monthly	Navi Mumbai

Configuration Audit

- No of Devices and Servers to be audited : 180
- 2 Initial SCA Test: Number of days.
- 2 Confirmatory SCA Test: Number of Days.
- Model : Onsite and / or Offsite
- Approach : Standard
- Report Discussion.
- Remediation Consulting.

Configuration of the in scope network-security & other devices

- The details all of the current network-security devices like firewall appliances, IPS appliances, Iron port appliances, Wi-Fi Controllers and access points, Access Control Server, routers and switches used by StockHolding in current Network are given in **Annexure A**. StockHolding may increase the number of in-scope devices during the tenure of the contract without any extra cost to StockHolding.
- The System Integrator is required to co-ordinate with the OEMs/partners in case of any hardware or software issue. The System Integrator has to take the sole responsibility to resolve the issue with OEM/partner. However, StockHolding will provide their support wherever required.
- In future StockHolding may go for the implementation of new type of devices / technologies like DAM, PIM, Application firewall etc. The System Integrator needs to maintain the configuration of the devices at no extra cost to StockHolding.
- The System Integrator is required to maintain basic configuration template for all devices i.e. firewall appliances, IPS appliances, Iron port appliances, Wi-Fi Controllers and access points, Access

Control Server, routers and switches etc. as per StockHolding's IT security policy and implement the same across the network to maintain the uniformity of the configuration.

- The System Integrator shall implement security policy, QOS policy and traffic reengineering policy that will be decided by StockHolding, change policies as per the requirement of StockHolding from time to time. The System Integrator shall coordinate with the service provider for its implementation and take complete ownership of the configuration.
- System Integrator to configure QOS on perimeter router as required to maintain the optimal quality of the application.
- The System Integrator is required to maintain the configuration on firewall appliances, IPS appliances, Iron port appliances, Wi-Fi Controllers and access points, internet routers and switches and required to do the changes in routing table, access-list, etc. as & when required to maintain the business function.
- The System Integrator has to ensure and enable end-to-end encryption to provide security in the data communications.
- The System Integrator is required to implement End-to-End Router based IPSec encryption (IPSEC /3 DES/AES) architecture for all existing and new / proposed locations and to DC and DR sites so as to encrypt the data flow based on the requirement of the applications deployed.
- The System Integrator is required to do the required configuration in the internet link terminating routers at DC at Mahape & DR at Bangalore.
- The System Integrator is required to conduct network drills at regular intervals (to be decided by StockHolding) for all devices configured in high availability mode by passing traffic through the devices which were in passive mode.

Network-Security functionalities / VA, PT and Configuration Audit

During the tenure of the contract, the System Integrator shall conduct a network-security audit twice in a year (every six months) on the following aspects without any cost to StockHolding:

- To examine the health of the network devices by verifying the parameters such as utilization during peak hours, version control of firewall appliances, IPS appliances, Iron port appliances, Wi-Fi Controllers, WAF Appliances, VPN Appliances and access points, routers and switches, Operating Systems of Servers and other network parameters/ applications/devices, Access Control Server etc.
- To identify the performance bottlenecks and to take suitable rectification steps, in consultation with StockHolding and suggest measures for improvement.
- The System Integrator will be responsible for configuration of the network-security devices as per StockHolding's IT security policy. StockHolding can conduct the audit of the network as per SEBI/RBI guidelines, if any or as per StockHolding's requirement through a third party or by StockHolding's Internal audit team on quarterly, half yearly and yearly basis.
- System Integrator will be responsible for complying with all the audit observations. The System Integrator has to ensure re-validation checks and post fix of the VA/Audit is performed, after the relevant configuration changes are made in the network, without any additional cost to StockHolding.

- System Integrator has to conduct periodic vulnerability assessment and penetration testing of the SIEM tool services provided as per StockHolding's IT security policy.

The System Integrator has to ensure review and rectification of the entire in-scope network-security devices configuration during contract period.

Backup & OS Management

- The System Integrator is required to take periodic backup of all network-security servers and devices as per StockHolding's IT policy and keep record of the same.
- The System Integrator is required to occasionally test the authenticity of the backup taken by restoring the same in the in-scope network devices.
- The System Integrator is required to take configuration backup before & after each change management activity as the same can be used for restoration in case of any issue post change management.
- The System Integrator is required to inform StockHolding is case of any requirement of IOS up gradation required in any of the network-security servers and devices and perform the same post approval from StockHolding.

OTHER SECURITY SERVICES

Security Intelligence Services

The System Integrator shall regularly track and advise StockHolding about new global security threats and Vulnerabilities. The advisories shall be customized to suit StockHolding's network and information security infrastructure. The System Integrator shall advise upgrades/ changes in the security infrastructure of StockHolding against evolving threats and vulnerabilities. Onsite team shall conduct impact analysis of new vulnerabilities and threats to StockHolding's assets and take necessary action on immediate basis for High and Medium Severity Vulnerabilities.

The System Integrator should advise and coordinate implementation of controls to mitigate new threats.

The System Integrator or their onsite team shall ensure adequate, appropriateness and concurrency of various policies and guidelines in place and shall provide Information Security consultancy for newer technology deployment for new and existing applications and products.

Onsite Team shall track and support implementation and coordinate for closure of vulnerabilities on assets that are affected. The System Integrator shall provide a security dashboard for online view of the global vulnerabilities and threats applicable to StockHolding's environment, number of assets affected and status of mitigation. Onsite team should take immediate

The System Integrator shall guide and recommend StockHolding with respect to any change required in the existing infrastructure of StockHolding for deployment of new application and services, which can have security implication to StockHolding, like- changing of rule in Firewall, Router, IPS, and application/ server configurations.

SOC team shall identify evolving vulnerabilities and threats to IT infrastructure assets, deployed in StockHolding. This includes

- Top global attack sources
- Top global attack targets
- New Vulnerabilities and advisories
- New Attack vectors
- Worms & Virus outbreaks

System Integrator should provide countermeasures, patches and recommended workarounds or Solution to remediate vulnerabilities as and when they are discovered for StockHolding IT Assets.

Security Advisory Services

- The System Integrator should regularly track and advise StockHolding about new global security threats and vulnerabilities.

- The advisories should be customized to suit StockHolding's security infrastructure. Advise upgrades / changes in the security infrastructure of StockHolding against evolving threats and vulnerabilities.

- The System Integrator shall providing Risk Assessment and Risk Treatment Services to StockHolding on yearly basis.

- The System Integrator shall assist StockHolding in formulation and review of various Policies and Plans, like- IT Security Policy, BCP-DR Plan, Cyber Fraud Policy, Digital Evidence Policy, Migration Policy, MDM Policy, Hardening Policy, and IS Audit Policy etc. The System Integrator shall also assist StockHolding in development of necessary procedures for the same.

- Evaluation of Information Security related audit observations of StockHolding and facilitating the rectification thereof.

- The System Integrator shall assist StockHolding in planning, execution, and implementation of information security related initiatives/projects/programs in StockHolding.

- The System Integrator shall assist StockHolding in development/review, monitoring, testing, and implementation of BCP and DR Planning related to network and network-security devices.

- The System Integrator shall participate in the periodic DC-DR Drill activity of StockHolding and suggest and assist in implementation of enhancements in the DC-DR Drill process related to network-security.

- For any new applications rollout by StockHolding, the System Integrator shall do network-security requirement assessment and advise StockHolding.

DELIVERABLES

System Integrator has to manage the SOC on 24X7X365 basis and deliver the services and provide the reports to StockHolding on periodic basis throughout the contract period for each of the services mentioned under project scope, in addition to providing other critical observations / methods/ improvements as deemed fit based on System Integrator’s professional experience for each of the services mentioned above.

- Integrate all the systems supplied with the Incident Management, change management, problem management and SLA management within Dashboard viewing system.
- Monitor and advise security incident on 24X7X365 basis to StockHolding and track the resolution of the same and close the incidents.
- Escalate the open incidents, as per the escalation matrix till resolution of the same.
- Take up the Vulnerability Assessment and penetration testing report and advise the mitigation steps to the concerned department of IT.
- Continuously fine tune the SIEM tool implementation to reduce false positives.
- Continuously improve the SOC operations to maximize the usage of tools.
- Provide secure web based incident management and dashboard facility to enable StockHolding to monitor the incidents status with drill down facility on various parameters.
- Manage archival of logs as per the Archival and retention policy of StockHolding.
- Provide 24X7X365 comprehensive maintenance support at DC and DR to resolve any technical problem/issues.
- Vulnerability Scanning and provide solutions to all the IT Assets (Servers, Network and network security appliances and devices scan initiated by SOC team with valid CVE ID for the vulnerabilities discovered and reported in the report as per the defined frequency.
- Remediation plan of deficiency observed in the VA has to be prepared by the onsite resource personnel.
- Provide the complete set of Operation and System Manuals in -3- sets of Hardcopies as well as in Softcopies of all the systems, components, network-security servers and devices managed and maintained as part of the SOC Operations.
- Define the SOC process manual.

Transition Management

StockHolding recognizes that the transition process and its effectiveness has a significant impact on the success of ongoing services. Transition involves one-time activities required to transfer responsibility for the services, including processes, assets, facilities, technology and other knowledge to the System Integrator. StockHolding has considered a transition period of 2 months from existing System Integrator to new System Integrator for smooth transfer of the SOC services handover process.

The System Integrator should ensure the smooth transfer of the services so as to continue to meet StockHolding's business requirements in a way that minimizes unplanned business interruptions. The System Integrator will be responsible for planning, preparing and submitting a Transition Plan to StockHolding. System Integrator will fully cooperate and work with any and all StockHolding's Third Party Contractors/Vendors/Consultant in a manner that will result in a seamless transfer of Services, and such transfer of Services shall be in accordance with the Transition Plan. During the Transition Period, System Integrator will be responsible for implementation of the Governance Model.

System Integrator will identify the suitable personnel for the roles defined under the governance structure for implementation. System Integrator will also be responsible for appointing its representative members to the newly established governance forums.

System Integrator will have the sole responsibility for implementation of the new System Integrator's delivery organization structure. All preparation and planning for such implementation must be completed during the Transition Period.

The System Integrator will explain how and when it will implement the transition activities, describe how it will transition Services from StockHolding's current environment. The System Integrator will include a project plan ("Transition Project Plan") indicating the tasks, timeframes, resources, and responsibilities associated with the transition activities.

System Integrator has to develop a detailed transition plan covering at least the following key areas:

- Transition Schedules, Tasks and Activities
- Transition activities
- Operations and Support
- Maintenance
- Resource Requirements
- Software Resources
- Hardware Resources
- Facilities
- Personnel
- Other Resources
- Relationships to StockHolding's other Teams / Projects

- Management Controls
- Reporting Procedures
- Risks and Contingencies- Key Risks, issues, dependencies and mitigation plans.
- Transition Team Information
- Transition Impact Statement and assessment
- Review Process
- Configuration Control
- Plan Approval
- Describe tools, methodologies and capabilities of the teams deployed for transition.

All System Integrators are required to ensure that their framework for transition of proposed services from StockHolding IT team/current Service Provider, at a minimum should include the following phases and allied activities:

Service Requirements	Description
Initiation	Kick off the transition based on the agreed transition plan
Planning	This phase takes care of all the planning activities required for successful transition of services
Execution	Execute the transition of services while ensuring near zero risk and no disruption to business.
Closure	Create all the transition documents and submit to the client for review and sign off and start off with MIS & SLA reporting.

System Integrator's Roles & Responsibility

S.No	**Tasks**
A	**Initiation**
1	Project kick-off
2	Team mobilization
B	**Planning**
3	Project charter
4	Communications plan
5	Set-up transition management process (risk, issues, changes, dependencies, reporting etc.)
6	Agreement on acceptance criteria and sign-offs
C	**Execution**
7	Discover and study existing practice, process, assets etc.
8	Define service delivery process
9	Define processes; develop SOPs, checklists, escalation matrix and flow charts. (System Integrator has to obtain StockHolding's sign off on documentation prior to completion of transition phase)
10	Deploy tools Monitoring tools as a service

11	Configuration of monitoring parameters and SLAs
12	Shadow support
D	**Transition Closure**
13	Primary Takeover
14	Business as usual to be delivered by successful System Integrator's operations team as per scope of work
15	Finalized run-books
16	Hand-over document
17	Finalize the Service transfer process document
18	Submit the Transition documents to StockHolding for review and sign off
19	MIS report generation and SLA reporting
20	The scope of work mentioned is illustrative and not exhaustive. The System Integrator needs to comply with StockHolding's requirements and any statutory or regulatory guidelines

- System Integrator to ensure proper documentation during each phase of transition and get them approved by StockHolding Networking team.
- Maintain steady operation of Transition period will have to be done within 30 days from the date of the order from the existing System Integrator
- System Integrator has to provide sufficient staff during the transition period however the payment for services shall start after the transition period and formal handover of service to the System Integrator.
- Finalize the reporting mechanism in consultation with StockHolding.

Periodic Review of the project

StockHolding officials will hold a meeting with the senior officials of selected System Integrator once in a Quarter or as decided by StockHolding on a later date to review the progress and to take necessary steps/decisions for performance improvement. The scope of the meeting includes but not limited to the following.

- Taking decisions on network-security architecture designs.
- Making necessary Policies/ changes as part of change management.
- Examining the level of SLA compliance achieved and taking steps for improvement.
- Attending to dispute resolution.
- Suggesting extra reports based on SLA requirement.
- Transition process planning.
- Health monitoring of the network-security appliances and devices
- Any other issues that arise from time to time.

Resource Management

All team resources included in SOC Operations and device management should be on the payroll of System Integrator. At least eight resources should be allocated for StockHolding for the full project contract duration as a Security Consultants. They should have professional qualifications like CISSP/ CEH/ CCSP/ CISA/ CISM or OEM Certified for the product/ solution. Resume/ CV for each of these members should be provided to StockHolding. They should have experience in a StockHolding/Financial Institution for SOC implementation / device management of at least 3 years each, with the Services/ Solutions mentioned in the RFP along with at least 2 years of experience with System Integrator. The System Integrator shall submit the proof of the experience.

On-site Manpower Assignment - Annexure – B

StockHolding has considered following man-power requirement as per our existing SOC setup manpower manage by existing vendor. However, System Integrator can go through all the activities requested in the RFP proposal and based on that they may add additional man-power, if required with a valid justification to be provided to StockHolding during presentation and accordingly they may include in the proposal to be submitted to StockHolding.
The System Integrator shall depute following minimum manpower at StockHolding site as given below:

S No	Location	Profile	No.	Service Window (24 * 7 * 365)
1	Mahape	Project Manager + Team Lead	1 + 1	09:00 AM to 06:00 PM
2.	Mahape	Security consultant	1	07:00 AM to 03:00 PM
3.	Mahape	Security consultant	1	11:00 AM to 07:00 PM
4.	Mahape	Security Consultant	1	01:00PM to 09:00 PM
5.	Mahape	Security Consultant	1	03.00 PM to 11:00 PM
6.	Mahape	Security Consultant	1	11.00 PM to 07:00 AM
7.	Mahape / Bangalore	Security Consultant	1	As decided by Stockholding. 09:00AM to 06:00PM

However, Shifts may change depending on the work requirements, the personnel deputed should be prepared to work long hours in case of emergencies.

The System Integrator has to ensure strict penal action is initiated, monetary OR suspension/dismissal, against onsite/shared resources deployed at StockHolding for any type of misconduct, misbehavior, mis-demeanor, in-subordination, moral turpitude exhibited while dealing with the officials/employees/contractors/vendors of StockHolding, in the course of discharging their duties at StockHolding.

The System Integrator on receipt of such an adverse remark, in writing OR during reviews conducted by StockHolding, should ensure compliance and submit a detailed action taken report (ATR) on their letter head to StockHolding.

Serial Number	Job Profile	Qualifications and Skills	Total Required Manpower
1	Security Consultants Location: Mahape DC – Navi Mumbai	• SIEM Certified/Trained. • CCSE / CEH Certified. • 3+ years experience in network-security device management / Information security and minimum 2 year of experience on payroll with System Integrator handling similar role in network-security. • Thorough knowledge of system administration of Windows, Linux, Unix and AIX platforms and networking and security devices like Firewalls, Web Application firewalls, IPS/IDS, Switches, Routers, ESA Spam mail Solutions, ISE Appliances, Load balancers, WAF, PIM, DAM, End to end Antivirus Management, End point antivirus management, NTP Server and Services Management, Proxy Management, VPN Gateways etc. management on standalone as well as on virtualized environment, on premises and on cloud (Private and/or Hybrid) • Experience in Event Correlation and Analysis • Experience in vulnerability assessments, Penetration testing. • Experience in handling events thrown by IPS, WAF, PIM and DAM tools and Spam Mail appliances. • Experience in patch management, configuration management. • Experience in implementation and management of security gateways, VPNs. • Thorough understanding of TCP/IP, networking concepts and internet protocols.	6

		Job Role • Managed Detection and Response Administration. Monitoring and analyzing the Critical, High, Medium and Low Severity tickets raised for the IT Assets integrated with MDR and closed the same by coordinating with respective IT Team as per SLA parameters. • Following up with MDR team from Call initiation till call closure in MDR Dashboard for all the IT assets integrated with MDR. • Incident Validation. • Detailed analysis of attacks and Incident Response. • Solution recommendation for IT Assets vulnerabilities. • Implementation of patches and secure configuration of servers. • Manage security devices. • Risk analysis for change management for security devices. • Escalation point for device issue resolution. • Resolve escalation. • Identify missed incidents. • Maintain knowledge base. • VA Tool administration.	
2	Project Manager + Tead Lead Location : Mahape DC – Navi Mumbai	• CISSP / CISM / CCSE / CEH Certified. • 5+ years experience in network-security device management / Information security and minimum 2 year of experience on payroll with System Integrator handling similar role in network-security / Information Security. • Certified in SIEM Tool being deployed. • Should have experience of WAF, PIM and DAM tools operations. • Comprehensive management experience in	1 + 1

		leading large scale security operations. • Experience in roll out of SIM, vulnerability management products. • Experience in setting up SOC processes • Domain experience in threats and vulnerabilities • Knowledge of system administration of Windows, Unix platforms and networking devices like Firewalls, IPS/IDS, Switches, Routers, Spam mail Solutions, ACS Appliances, Load balancers, WAF, PIM, DAM, End to end Antivirus Management, NTP Server and Services Management, Proxy Management, VPN Gateways etc. • Thorough understanding of TCP/IP, networking concepts. • **Job Role** • Managed Detection and Response Administration. Monitoring and analyzing the High and Medium Severity tickets raised for the IT Assets integrated with MDR. • Track Incident detection and reporting. • Incident closure. • Incident escalation. • Identify new alert requirement. • Ensure services are being provided within SLA parameters. • Performing periodic DR drill. • Follow-up up departments for closure of various reports / Incidents and escalate the long outstanding issues / Change Management / Problem Management.	

In case of exigencies, Security consultants and project manager should be available on Sundays and Holidays as well.

In case of absence of any of the resource person, standby manpower should be provided by the System Integrator. If StockHolding is not satisfied with the performance of the standby personnel, StockHolding may not accept such standby manpower and in such cases, charges on actual basis of manpower support will be charged to the System Integrator subject to adherence of SLA conditions. The above details are only indicative figures and may undergo change as per the requirement of StockHolding from time to time.

StockHolding may conduct interview of each of the System Integrator's selected resource before deployment in the project. A Technical Program Manager shall be appointed & be responsible for execution and compliance of entire Scope of Work. Although the Technical Program Manager for the project would not be stationed at StockHolding, but he or she shall be required to visit StockHolding for attending the meetings, taking feedback, review of policies, consultation etc. and giving recommendations there of as and when required by StockHolding as well as to meet the project requirement.

The Technical Project Manager shall visit StockHolding at least 2 times per month or as directed by StockHolding officials to review the project. The number of visits may increase during important activities or as and when required.

System Integrator and the personnel's deployed for SOC Operation and device management having access to information on StockHolding's security programs and systems received or generated under this contract shall ensure that they meet StockHolding's requirements.

System Integrator shall conduct adequate background checks of the personnel who will be deputed at positions handling StockHolding's sensitive information. System Integrator shall submit an undertaking that they have conducted adequate background screening of their employees who will be assigned for this project. The background check report for each personal deputed at StockHolding's site has to be submitted to StockHolding on quarterly basis till the contract expiration period.

- System Integrator shall maintain confidentiality of StockHolding's information accessed by them.
- System Integrator shall sign Confidentiality cum Non-Disclosure Agreement on behalf of all such employees.
- Once System Integrators' personnel are removed from the project, whether on termination / resignation etc. the same should be immediately informed to StockHolding and preclude any further access to all information to such person. Prior approval should be obtained from StockHolding before granting access to StockHolding's information either at System Integrator's site or at StockHolding's sites.

System Integrator should not transfer any of its onsite resources from StockHolding's premises within 12 months of deployment without written consent of the designated StockHolding official. In case of inevitable circumstances, System Integrator shall deploy an eligible employee with an equivalent or higher work experience at least one month prior to replacement of the deployed resource.

StockHolding will impose a penalty at a rate of 10% of its total monthly payable for each case of such violation.

SERVICE LEVEL AGREEMENT AND PENALTY:

The System Integrator needs to execute a Service Level Agreement with StockHolding covering all terms and conditions of this tender. System Integrator need to strictly adhere to Service Level Agreements (SLA). Services delivered by System Integrator should comply with the SLA mentioned in the table below.

The System Integrator should generate SLA reports for tracking the delivery of services. SLA will be reviewed on a monthly basis and based on the review payments for the services will be done. Thus enabling StockHolding to continuously track the SLA.

The SLA violation will attract penalties as per the terms of the RFP.

Service Level Targets Metric Calculation and Penalty Calculation
High level service level targets are described in sections below.

Service Level Agreement (SLA)

1. SLA deviation calculation to be considered on monthly basis.
2. The penalty will be calculated on the monthly contract value.
3. The total cap on monthly penalty is 15% of the monthly contract value and the overall cap on penalty is as follows:

A. Monitoring and Management of Network Devices

Uptime Commitment for Network Security Devices.

Parameter	Metric	SLA	Metric Calculation	Unit of Measure	Reporting Frequency	Bench Mark
Uptime	Uptime of all In-Scope devices.	SLA	Total no. of hours the in-scope devices are unavailable.	Percentage - As per severity of devices	Monthly	Very High >=99.5%, High >=98%, Medium >=98%

Business Hours Window: (24 * 7 * 365 Support = 24 hours in a day * 30 days = 720 hours.
System Integrator should provide average system/solution uptime of 99% and 98% device specific on the entire Bill of Material as per “Network equipment uptime” table as shown above on monthly basis.

Uptime shall be calculated at the end of each month as follows.

Uptime: {(Actual Uptime in Hrs. – Downtime in Hrs.) / Schedule Hrs.} x 100

A. Actual Uptime means, of the scheduled hours, the aggregate number of hours in any month during which each defined and supported equipment is actually available for use.

B. Downtime in Hrs. means the aggregate number of hours in any month during which each defined and supported equipment and service is down during scheduled hours other than due to preventive maintenance, scheduled outages, Upgrades and updates, LAN cabling faults, infrastructure problems or any other situation which is not attributable to System Integrator's failure to exercise due care in performing its responsibilities.

C. Scheduled hours means the days of the week and the hours per day for which the System Integrator has committed to an availability service level for a system or network and during which periods such Availability Service Level will apply.

B. Configuration and Capacity Management of Network Devices.

Event	Criticality	Timeframe	Benchmark	Penalty Calculation
Create, modify and delete configurations in network devices after obtaining approval from the StockHolding Team.	As per device / Application risk severity rating.	Response Time : 30 min	Resolution time: 2 hour	For each instance of breach, *penalty of 1% up to 2 Hrs. Above 2 Hrs. and less than 4 Hrs. additional 1 %, And above 4 hours 5% Subject to total cost of monthly Invoice cap.*
Review of capacity planning of in scope network and network-security devices, appliances and Servers.	As per device / Application risk severity rating.	Response: starting on the 1st day of the first month of the Start of every Quarter.	Resolution: within 5th day of the first month of the start of every Quarter.	For every 1 week of delay or part thereof, the *penalty of 1% of the total cost of monthly invoice value/week basis till resolution.*
Loss of any network assets, under the control of the service providers' onsite team, due to omission or negligence or failure, to follow the due process in handling and updating the network inventory.	High			For each instance of breach, penalty will be INR 5,000, in addition, the purchase value of the lost asset at that period of time will be Recovered.

Deviation of every instance from the benchmark will attract a penalty of 5% of the total cost monthly invoice value (max up to 15% of monthly billing). Penalty will be calculated on a monthly basis post verification of monthly report.

C. Incident Management and Investigation Metric Calculation and Penalty

Incident Management aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service-quality are maintained. 'Normal service operation' is defined here as service operation within service level agreement limits.

Incident management can be defined as any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service.

The objective of incident management is to restore normal operations as quickly as possible with the least possible impact.

Parameter	Metric	SLA	Metric Calculation	Unit of Measure	Reporting Frequency	Bench Mark
Response Time	% of Tickets responded within the SLA	SLA	Total number of Tickets responded within SLA by total number of Tickets handled by the SOC team.	Percentage - As per severity of devices	Monthly	Very High >=99% within 30 Minutes, High >=99% within 60 Minutes, Medium >=99% within 2 Hours, Low >=99% within 4 Hours.
Resolution Time	% of Tickets resolved within the SLA	SLA	Total number of Tickets resolved within SLA by total number of Tickets handled by the SOC team.	Percentage	Monthly	Very High >=99% within 2 Hours, High >=95% within 4 Hours, Medium >=95% within 12 Hours, Low>=95% within 48 Hours

Event	Criticality	Timeframe	Reporting Frequency	Penalty Calculation

Call/Ticket logging to OEM/SI/Vendor for device malfunctioning (call should not be rejected by OEM/SI/Vendor citing configuration issue)	Medium	Response time-30 min	Monthly	For each instance of breach, penalty will be INR 5,000 per day till Call logging

D. Resource Management

Event	Criticality	Penalty Calculation
Unavailability of resource on site.	High	For each instance of breach, penalty will be INR 5,000
Late Coming/Early departures will be considered as absent for the day.	High	For each instance of breach/resource, penalty will be INR 5,000
The full resource strength as agreed in the PO should be deployed onsite per day per month for the entire contract period.	High	For each instance of breach/resource, penalty will be INR 5,000
Separation of duties (i.e. use of email ids and login ids across roles)	Medium	For each instance of breach/resource, penalty will be INR 1,000
Additional certified skilled resource/s having greater expertise/skillsets/knowledge than the incumbent onsite team should be deployed, to supplement the efforts of the on-site support team during emergencies and contingencies (i.e. for incidents/events bearing severe impact on systems under scope)	High	For each instance of breach, penalty will be INR 5,000/day till resolution is made, capped at 15% of monthly invoice.
Any/All, trainings aligned for the onsite resources of the service provider, should be intimated by the SP backend team (program manager or equivalent and above) in advance of at least 2 weeks in writing for approvals from the StockHolding team, along with the necessary provisioning plan for a shadow/backup resource -in line with the PO OR having greater expertise/knowledge/skillsets and qualification / OEM Certification- to be deployed onsite in the event of the original resources being not available for the said training period.	High	

E. Problem Management

Problem management aims to resolve the root cause of incidents to minimize the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. A 'problem' is an unknown underlying cause of one or more incidents, and a 'known error' is a problem that is successfully diagnosed and for which either a workaround or a permanent fix has been identified.

A problem is a condition often identified as a result of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant.
A known error is a condition identified by successful diagnosis of the root cause of a problem, and the subsequent development of a work-around.

The principal purpose of *problem management* is to find and resolve the root cause of a problem and thus prevent further incidents; the purpose of *incident management* is to return the service to normal level as soon as possible, with smallest possible business impact.

Parameter	Metric	SLA	Metric Calculation	Unit of Measure	Reporting Frequency	Bench Mark
Root Cause	% of RCA report submitted (Critical)	SLA	Total number of RCAs submitted within 48Hrs./ Total number of RCAs	Percentage	Monthly	>95%

Note: Deviation of every 1% from the benchmark will attract a penalty of 3% of the cost of monthly invoice ***(max up to 15% of monthly billing).*** *Penalty will be calculated on a monthly basis post verification of monthly Incident reports.*

F. Change Management

Change management aims to ensure that standardized methods and procedures are used for efficient handling of all changes; a change is "an event that results in a new status of one or more configuration items approved by management and enhances business process changes (fixes) - with a minimum risk to IT infrastructure.

The main aims of change management include:

- Minimal disruption of services
- Reduction in back-out activities.
- Economic utilization of resources involved in the change

Change Management Terminology

- Change: the addition, modification or removal of CIs
- Forward Schedule of Changes (FSC): schedule that contains details of all forthcoming changes.

Parameter	Metric	SLA	Metric Calculation	Unit of Measure	Reporting Frequency	Bench Mark
Schedule Adherence	Schedule Adherence – Change	SLA	Total number of Changes Implemented by total number of changes planned for the month	Percentage	Monthly	>=95%
Change Management Efficiency	Successful Changes	SLA	Total number of Changes implemented successfully by total number of changes implemented	Percentage	Monthly	>=95%
Failed Changes	% changes rolled back	SLA	Total number of changed rolled back due to failure by total number of changes implemented successfully	Percentage	Monthly	<=5%

Deviation of every 1% from the benchmark will attract a penalty of 3% of the cost of monthly invoice (max up to 15% of monthly billing). Penalty will be calculated on a monthly basis post verification of change management details on monthly basis.

G. Compliance Management Terminology and Action from SOC Team.

(Applicable for Audits / Configuration Audits / Vulnerability Assessment and Penetration Testing / Secure Network Architecture / Remote Assessment / Red Team Assessments / Monthly Security Advisories – CERT-in, NCIIPC, SEBI, NSDL, CDSL, PFRDA, IRDA and RBI etc. closures for the observations reported by them.)

- Compliance action : The addition, modification of changes.
- Forward Schedule of Changes (FSC): schedule that contains details of all forthcoming changes.
- Vulnerability Assessment and Penetration Testing reports (Internal and external) can be provided to SOC team on quarterly basis by respective internal and external vendors. Analysis and action taken to be completed on such VA/PT in the 1st month for “Critical” and “High” severity vulnerabilities. Post Medium severity vulnerabilities to be close in the 2nd month. All the “Low” Severity vulnerabilities to be close in 3rd month i.e. Before Initiating the confirmatory test for VA/PT from respective vendor.
- Internal and external audit related findings to be close on priority basis within a stipulated period provided by StockHolding.

Parameter	Metric	SLA	Metric Calculation	Unit of Measure	Reporting Frequency	Bench Mark
Schedule Adherence	Schedule Adherence – Change	SLA	Total number of Changes in compliance Implemented by total number of changes planned for the month.	Percentage	Monthly	>=95%
Changes in Compliance Management Efficiency	Successful Changes	SLA	Total number of Changes in compliance implemented successfully by total number of changes implemented.	Percentage	Monthly	>=95%
Failed Changes in Compliance Management.	% changes rolled back	SLA	Total number of changed rolled back due to failure by total number of changes implemented successfully.	Percentage	Monthly	<=5%

Deviation of every 1% from the benchmark will attract a penalty of 3% of the cost of monthly invoice charges (max up to 15% of monthly billing). Penalty will be calculated on a monthly basis post verification of monthly compliance report.

SOC Operations:

Serial Number	Service Area	Criticality	Service Level
1	Network-Security device management and monitoring.	Most Critical	• 24x7x365 device management / event / log monitoring and correlation. • Event alerts within 5 minutes of the event. • Initiate response/Incident generation within 15 minutes • Mitigation of security events / threats. • Availability of relevant logs online for last 3 months. • Real time dashboard view. • Daily reports before 10:00AM • Weekly report as on the specified day (Example: On Monday) before 10:00AM. • Monthly consolidated report by 7th of

			every month. • Monthly Reports Standard / Exception reports.
2	Dedicated Onsite Resources as per Annexure - B	Critical	As per roles and responsibilities mentioned under Annexure B
3	Security Intelligence Services and Reports.	Important	Advisories within 12 hours of new global threats & vulnerabilities disclosures.

Expected SLA for network-security devices:

Sr. No.	Activity	Service Parameter	SLA
1	Managed firewall Services	System Availability.	24x7x365
		Response time for advising StockHolding regarding policy violation.	Immediate
		Response time for advising StockHolding regarding device downtime.	15 min
		Resolution time for reconfiguration and Closure.	30 min
		Periodicity of firewall security policy review-Change Report.	Weekly
2.	Managed ISS Services + Site protector	System Availability.	24x7x365
		Response time for advising StockHolding regarding policy violation.	Immediate
		Response time for advising StockHolding regarding device downtime.	15 min
		Resolution time for reconfiguration and Closure.	30 min
		Periodicity of IPS security policy review-Change Report	Weekly
3.	Managed Incident Detection and Response services.	Response time for advising StockHolding on detection of an incident.	15 min
		Severity based response time for forensics and for undertaking counteraction for blocking the Incident.	Immediate

4.	Managed Switch Services.	System Availability.	24x7x365
		Response time for advising StockHolding regarding device downtime.	15 min
		Resolution time for reconfiguration	30 min
		Periodicity of switch security policy review-Change Report	Monthly
5.	Managed Router Services.	System Availability.	24x7x365
		Response time for advising StockHolding regarding device downtime.	15 min
		Resolution time for reconfiguration	30 min
		Periodicity of Internet router security policy review-Change Report	Monthly
6.	Managed Proxy Services.	System Availability.	24x7x365
		Response time for advising StockHolding regarding device downtime.	15 min
		Resolution time for reconfiguration	30 min
		Periodicity of Proxy security policy review-Change Report	Monthly
7.	Managed Websense Services	System Availability.	24x7x365
		Response time for advising StockHolding regarding software downtime.	15 min
		Resolution time for reconfiguration	30 min
		Periodicity of websense security policy review-Change Report	Monthly
8.	Managed Iron port Appliances Services	System Availability.	24x7x365
		Response time for advising StockHolding regarding services downtime.	15 min
		Resolution time for reconfiguration	30 min
		Periodicity of Iron port security policy review-Change Report	Monthly
9.	Managed Wireless Controller Services	System Availability.	24x7x365
		Response time for advising StockHolding regarding services downtime.	15 min

		Resolution time for reconfiguration	30 min
		Periodicity of Wireless Controller security policy review-Change Report	Monthly
10	Managed ACS Services	System Availability.	24x7x365
		Response time for advising StockHolding regarding services downtime.	15 min
		Resolution time for reconfiguration	30 min
		Periodicity of ACS security policy review-Change Report	Monthly
11	Managed DDoS Services	Link Availability.	24x7x365
		Response time for advising StockHolding regarding link downtime.	15 min
		Resolution time for coordination and closure	30 min
		Periodicity of mDDoS Services Review	Monthly
12.	Managed Internet Services.	Link Availability.	24x7x365
		Response time for advising StockHolding regarding link downtime.	Immediate
		Resolution time for coordination and closure	30 min
		Periodicity of ACS security policy review-Change Report	Monthly

Expected reports along with Analysis from System Integrator.

S/N.	Activity	Reports	Frequency
1	Firewall Appliances	Top 10 Inbound Allowed Traffic by IP Destination Address and analysis done and action taken by System Integrator.	Daily
		Top 10 Inbound Allowed Traffic by IP Destination. Port and analysis done and action taken by System Integrator.	Daily
		Top 10 Inbound Denied Traffic by IP Destination Port and analysis done and action taken by System Integrator.	Daily
		Top 10 Inbound Denied Traffic by IP Source Address and	Daily

		analysis done and action taken by System Integrator.	
		Top 10 Outbound Allowed Traffic by IP Destination Port and analysis done and action taken by System Integrator.	Daily
		Top 10 Outbound Denied Traffic by IP Destination Address and analysis done and action taken by System Integrator.	Daily
		Top 10 Outbound Denied Traffic by IP Destination Port and analysis done and action taken by System Integrator.	Daily
		Top 10 Outbound Denied Traffic by IP Source Address and analysis done and action taken by System Integrator.	Daily
		Top 10 Outbound Allowed Traffic by IP Source Address and analysis done and action taken by System Integrator.	Daily
		Top 10 Inbound Denied Traffic by IP Destination Address and analysis done and action taken by System Integrator.	Daily
2.	IPS Appliances + Site protector	Top 10 Events by Signature and analysis done and action taken by System Integrator.	Daily
		Top 10 Inbound Events by IP Destination Address and analysis done and action taken by System Integrator.	Daily
		Top 10 Inbound Events by IP Destination Port and analysis done and action taken by System Integrator.	Daily
		Top 10 Inbound Events by IP Source Address and analysis done and action taken by System Integrator.	Daily
		Top 10 Outbound Events by IP Destination Address and analysis done and action taken by System Integrator.	Daily
		Top 10 Outbound Events by IP Destination Port and analysis done and action taken by System Integrator.	Daily
		Top 10 Outbound Events by IP Source Address and analysis done and action taken by System Integrator.	Daily
3.	Cisco FMC and FPD appliance.	Top 20 Accepted Events by Destination Address and analysis done and action taken by System Integrator.	Daily
		Top 20 Accepted Events by Destination Port and analysis done and action taken by System Integrator.	Daily
		Top 20 denied Events by Destination Address and analysis done and action taken by System Integrator.	Daily
		Top 20 denied Events by Destination port and analysis done and action taken by System Integrator.	Daily
4.	Proxy + URL	Spyware Activity Summary and analysis done and action	Daily

	filtering.	taken by System Integrator.	
		Top Sites by Bandwidth and analysis done and action taken by System Integrator.	Daily
		Top Sites by Browse Time and analysis done and action taken by System Integrator.	Daily
		Top Users by Bandwidth and analysis done and action taken by System Integrator.	Daily
		Top Users by Browse Time and analysis done and action taken by System Integrator.	Daily
5	Antivirus Reports	Daily Antivirus Outdated client list Report and analysis done and action taken by System Integrator.	Daily
		Weekly Antivirus Outdated client list Report and analysis done and action taken by System Integrator.	Weekly
6.	Real Time reporting – Alerts view security	Denied Inbound / Outbound connection. (At the end of the day) and analysis done and action taken by System Integrator.	Real Time
		Severity Summary (At the end of the day) and analysis done and action taken by System Integrator.	Real Time
		Top Intruders (At the end of the day) and analysis done and action taken by System Integrator.	Real Time
		Top Attacks (At the end of the day) and analysis done and action taken by System Integrator.	Real Time
		Suspected Security Issues. (At the end of the day) and analysis done and action taken by System Integrator.	Real Time
		Attack Identification report. (At the end of the day) and analysis done and action taken by System Integrator.	Real Time
7.	Other Reports	Vulnerability Assessment / PT Services. (Internal Security Assessment Services.) and analysis done and action taken by System Integrator.	Half-yearly Analysis and Reports.
		Vulnerability Assessment / PT Services. (External Security Assessment Services. – Through Vendors office) and analysis done and action taken by System Integrator.	Half-yearly Analysis and Reports.
		Vulnerability- Action Taken Report	Half Yearly
8.	Process Reviews.		
	Tactical Review	Project Feedback / SLA Review.	Quarterly.
		Escalations and Service Improvements.	Quarterly.
	Operational Review	Activity Review and deadline tracking.	Monthly.

		Technical and Resource Issues.	Monthly.

Failure to generate and submit the report before 10:00 am daily for daily reports,
10:00 am on every first working day of the week for the weekly reports and
10:00 am on every 7th day of the month for monthly reports will be treated as failure to maintain the SLA and appropriate penalty will be levied by StockHolding.

Service review:
System Integrator should conduct external vulnerability security audit twice in a year.
System Integrator will provide their technical and management escalation matrix in the enclosed format.
Escalation matrix

No.	Description	Personnel	Email/Type	Contact
1	Level-1			Low: 24 Hrs. Report and resolve
2	Level-2			Medium: =<04 Hrs. to <02 Hrs.
3	Level-3			High / Critical: =<01 Hrs.

Managed Detection and Response and Other Services:

Serial Number	**Service Area**	**Criticality**	**Service Level**
1.	24x7x365 days Security Log Monitoring Services of in scope Devices management and Arcsight (SIEM service).	• 24x7x365 monitoring of security events to detect all internal & external attacks and action on raise the alerts by MDR Team for any suspicious events Incident. • **Initial response should be Initiated by SOC team after notification from MDR Team** a) Within 15 minutes for Critical (P0) and high priority (P1) incidents for all In-scope and other devices. b) Within 30 minutes for others (P2) priority incidents for all In-scope and other devices. • **Closure of raised alert. To be Closed after completing investigating by MDR Team** a) Within 30 Minutes for Critical priority (P0) events for all In-scope devices. Follow-ups for other	The penalty for breach of SLA will be as follows: - Very high and high priority alerts and notifications: 3% of monthly invoice value/ instance for in-scope devices. - Medium priority Alerts and notifications: 2% of monthly invoice value/ instance for in-scope devices. - Low priority Alerts and notifications: 1% of monthly invoice value/ instance for in-scope devices.

2.	Other Services.	devices not under control of SOC team, but follow-ups to be taken till closure by coordinating with respective team. b) Within 60 Minutes for High priority (P1) events for all In-scope devices. Follow-ups for other devices not under control of SOC team, but follow-ups to be taken till closure by coordinating with respective team. c) Within 90 minutes for Others (P2) priority events for all In-scope devices. Follow-ups for other devices not under control of SOC team, but follow-ups to be taken till closure by coordinating with respective team. • **Agreed/customizable daily & Monthly reports** should be submitted on next day prior 10:00AM and by 15th of subsequent month Respectively. • **Review of firewall rule base, IPS signatures of in-scope security devices** should be submitted to us on monthly basis or before 7thof the same month and needs to be completed the final action taken report by 30th of the subsequent month. • **Review of audit logs** should Be completed and after verification by StockHolding official, published on dashboard before 07th of the subsequent month on quarterly basis.	
2.	Anti-Malware and Anti Trojan	• Alerts generated from monitoring and detection systems should be	The penalty for breach of SLA will be as follows:

	scanning Services	suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident. • SOC team should have implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information to external parties. • The response and recovery plan of the SOC team should have plans for the timely restoration of systems affected by incidents of cyber- attacks or breaches • Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.	- Alert within 15 minutes For code injection attempts and attacks: 1% of monthly invoice value / hour of delay for every Instance. Initial remedial response within 30 minutes with action plan on locking/ containment/ recovery: 2% of monthly invoice value / 2 hours of delay for every Instance . - Resolution within 60 minutes: 2% of monthly invoice value / 2 hours of delay for every Instance
3	Security Intelligence	Advisories within 12 hours of vulnerability disclosure/global threat detection. Initiation & Resolution of remedial/ mitigatory measures to thwart such security vulnerabilities within 24 hours.	A delay of more than 24 hours will incur a penalty of 1% of monthly invoice value to be calculated on monthly basis for all the advisories reported in a month.
4.	Periodic Review	The System Integrator is expected to conduct a monthly review meeting with StockHolding officials resulting in a report covering details about current SOC SLAs, status of operations, key threats	Monthly meeting to be conducted on or before the 25th (tentatively) of each month. A delay of more than three days will incur a penalty of

		and new threats identified, issues and challenges etc.	1% of monthly invoice value.

Exit clause

StockHolding reserves the right to terminate this Agreement by giving 3 months' notice, if it is not satisfied with the Services. Reasonable number of incidents of the non-performance of the obligations by as per this Agreement will be provided before the termination notice is served on the. In case of termination, payments due till the date of termination only would be paid. Balance payment for remaining Agreement Term will not be paid to the System Integrator.

Due Diligence:

The System Integrator is expected to examine all instructions, Forms, Terms, Conditions and Specifications in this RFP. Bids shall be deemed to have been made after careful study and examination of this RFP with full understanding of its Implications. The Bid should be precise, complete with all details required as per this RFP document. Failure to furnish all information required by this RFP or submission of Bid not as per RFP requirements will be at the System Integrator's risk and may result in rejection of the bid and the decision of *StockHolding* in this regard will be final and conclusive and binding.

Cost of Bidding:

The System Integrator shall bear all costs associated with the preparation & submission of its bid and *StockHolding* will in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

Contents of this RFP Document:

The requirements, bidding procedure, general terms & conditions are prescribed in this RFP document with various sections

(A) Bids Preparation and Submission Details
(B) Requirement with Detail Scope of Work, and Terms and Conditions
(C) Service Level Agreements and penalties, Deliverables
(C) Format for Technical Bid - Annexure-3
(D) Format for Final no regret Commercial Bid - Annexure-4
(E) Form for entering EMD details - Annexure-5
(F) Integrity Pact - Annexure-7
(G) Compliance Statement Annexure-8

Clarifications regarding RFP Document:

- Before bidding, the System Integrators are requested to carefully examine the RFP Document and the Terms and Conditions specified therein, and if there appears to be any ambiguity, contradictions, gap(s) and/or discrepancy in the RFP Document, they should forthwith refer the matter to *StockHolding* for necessary clarifications.
- A System Integrator requiring any clarification for their queries on this RFP may obtain clarification via email to PRIT@StockHolding.com
- *StockHolding* shall not be responsible for any external agency delays.

- *StockHolding* reserves the sole right for carrying out any amendments / modifications / changes in the bidding process including any addendum to this entire RFP
- At any time before the deadline for submission of bids / offers, *StockHolding* may, for any reason whatsoever, whether at its own initiative or in response to a clarification requested by System Integrators, modify this RFP Document.
- All System Integrators who have received this RFP document shall be notified of the amendment on e-mail, and all such amendment(s) shall be binding on them
- *StockHolding* reserves the rights to extend the deadline for the submission of bids, if required. However, no request from the System Integrators for extending the deadline for submission of bids, shall be binding on *StockHolding*.
- *StockHolding* reserves the right to amend / cancel / postpone the RFP without assigning any reasons.

Bids Preparation and Submission Details

1. **Technical Bid**
   a. The System Integrator will submit the Technical Bid online on **https://stockholding.auctiontiger.net** and should be as per the format given (Technical Bid for Managed Security Services for Security Operation Centre - refer **Annexure-3**
   b. There should not be any hidden / conditional costs in the bids and in the event of their presence in the bid, the bid is liable to be rejected.
   c. No indications pertaining to price or commercial terms should be made in the Technical Bid submission. If any price indications are made, then the bids may be rejected.
   d. No open ended / conditional bid shall be entertained and are liable for rejection.
   e. System Integrator should submit scan copy of cancelled cheque for bank information required during returning EMD payment.

2. **Final No regret Commercial Bid**
   a. The System Integrator will submit Commercial Bid online on **https://stockholding.auctiontiger.net** as per the format given (Commercial Bid for Managed Security Services for Security Operation Centre - refer **Annexure-4**

3. **Submission of Bids**
   a. The required documents for Eligibility Criteria and Technical Bid, Commercial Bid must be submitted (uploaded) online on **https://stockholding.auctiontiger.net**. Technical Bid and Commercial Bid should be complete in all respects and contain all information asked for in this RFP document
   b. If Interest Free Earnest Money Deposit (EMD) is not submitted by System Integrator / received by StockHolding in the form NEFT/RTGS prior to the last date of submission of bids as mentioned in this RFP, System Integrator will not be eligible to participate in this RFP.
   c. The System Integrator shall fulfil all statutory requirements as described by the law and Government notices. The System Integrator shall be solely responsible for any failure to fulfil the statutory obligations and shall indemnify *StockHolding* against all such liabilities, which are likely to arise out of the agency’s failure to fulfil such statutory obligations
   d. The System Integrator shall be solely responsible either for any injury, damage, accident to the workman employed by the System Integrator for any loss or damage to the equipment/property in the areas of work as a result of negligence/carelessness of its deployed resources.

e. The System Integrators are requested to note that it is mandatory to have a valid digital certificate issued by any valid certifying authority approved by Govt. of India to participate in the online bidding. The System Integrators are requested to ensure that they have valid digital certificate well in advance or if any assistance is required for the purpose, System Integrators can contact service provider (M/s e-Procurement Technologies Ltd.).

Minimum requirement for e-Bidding:

1. Computer / Laptop (Notebook) with Internet connection
2. Operating system - Windows XP Service pack -3 / VISTA/ Windows 7 or above
3. Digital certificate - Class II or III, Signing + Encryption

Validity of offer:
The offer should remain valid for a period of at least 90 days from the date of submission

4. Evaluation of Bids

StockHolding will evaluate the bid submitted by the System Integrators under this RFP. It is *StockHolding*'s discretion to decide at the relevant point of time. The eligibility bid submitted by the System Integrator will be evaluated against the Eligibility criteria set forth in the RFP. The System Integrator needs to comply with all the eligibility criteria mentioned in the RFP to be evaluated for evaluation. Non-compliance to any of the mentioned criteria would result in outright rejection of the System Integrator's proposal. The decision of *StockHolding* would be final and binding on all the System Integrators to this document. *StockHolding* may accept or reject an offer without assigning any reason what so ever. Only those System Integrators who qualify all eligibility Criteria requirements will be qualified for technical bid evaluation.

Please note that all the information desired needs to be provided. Incomplete information may lead to non-consideration of the proposal.

Evaluation of Technical Bids
The Technical Bid submitted by the System Integrator will be evaluated against Evaluation parameters/Credentials set forth in RFP. Any System Integrator who satisfies all technical eligibility criteria and receives the cutoff marks of 70% and above shall be considered as *technically qualified* and will be considered eligible for participating in the Commercial bidding. No additional or preferential weightage based on Technical scores will be allocated to any of the technically qualified System Integrators.

Evaluation of Commercial Bids
StockHolding will intimate all System Integrators who are technically qualified on StockHolding website and on email *prior* to opening of commercial bids but *after* the final submission of the commercial bids. All System Integrators need to submit “sealed commercial bids” online on the

portal https://stockholding.auctiontiger.net with their final no regret commercial bid by the specified date and time. No bids can be uploaded after the cut-off time.

Commercial bids will be opened online on the portal only on the pre-specified date and time and bids received will be displayed on the portal by Auction Tiger. The lowest System Integrator will be considered by StockHolding for award of contract.

StockHolding reserves the right to negotiate price

- with the lone System Integrator or
- with the L1 System Integrator in exceptional circumstances like quote of unrealistic or unjustified prices

Payment Terms and Conditions

(1) Payment**:**

(a) Monthly payment on completion of deliverables & on submission of invoice
(b) Applicable penalty will / may be recovered from the monthly payment.
(c) Applicable TDS and/or CESS will be recovered (deducted) from the payment.
(d) First monthly Payment will be released only after signing of Integrity Pact and Non-Disclosure Agreement.

(2) Refund of Earnest Money Deposit (EMD)

(a) EMD will be refunded through NEFT to the successful System Integrator on providing an acceptance confirmation of PO given to System Integrator.

(b)In case of unsuccessful System Integrators, the EMD will be refunded to them through NEFT within 15 days after the commercial bid opening

(c)In case of unsuccessful System Integrator in technical round, the EMD will be refunded to them through NEFT within 15 working days of opening of technical bid

(3) Contract Period

Three years from the date of purchase order or formal confirmation of service

(4) Taxes & levies

(a) Applicable taxes payable at actual as per prevailing rate of taxes as per Government notification
(b) Applicable TDS may be recovered (deducted) from the payment(s)

(5) Penalty

Applicable penalty is as per scope of work and will / may be recovered from the payment(s)
This above-mentioned penalty may / will be deducted (recovered) against non-adherence of scope of work / deliverables.

However, the penalty may / will be waived off for non-performance due to reasons mentioned in the Force Majeure or because of StockHolding. In such case(s) the System Integrator should notify and produce / bring the relevant communication and proof to StockHolding promptly of any failure to perform or delay in performing due to any of the above reasons for the penalty to be waived off

(6) Force Majeure

The System Integrator will not be held responsible for breach of executing any obligation or delay in executing any obligations during below given circumstances / conditions:

(a) War, Riots, Strike, Fire, Flood, Earthquake, Storm, Epidemic/Pandemic breakout, Power failure, Theft etc.

(b) Any Governmental priorities (Necessary proof for validation viz. Govt. Gazette notifications, Leading Newspaper reports, etc. should be made available)

(c) Sabotage or omission of *StockHolding*

(7) Dispute Resolution:

In the event of any dispute arising out of or in connection with this Order, the parties shall use their best endeavour to resolve the same amicably AND if the dispute could not be settled amicably, the matter shall be settled in the court under Mumbai jurisdiction only. The final payment will be released only after the System Integrator complies with above-mentioned clause

(8) Right to alter RFP

(a) StockHolding reserves the right to alter the RFP terms and conditions at any time before submission of the bids.

(b) StockHolding reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever.

StockHolding's decision in this regard will be final and binding on all System Integrators.

(9) Integrity Pact

The System Integrator will have to enter in to an Integrity Pact with StockHolding Corporation of India Limited. The format (text) for the Integrity Pact is provided as **Annexure-7.** The successful System Integrator will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory of the successful System Integrator.

(10) Non-Disclosure Agreement (NDA)

The successful System Integrator will sign a Non-Disclosure Agreement (NDA) with StockHolding. The draft text of the NDA will have to be approved by legal department of StockHolding.

(11) No Commitment to accept lowest or any other bid

StockHolding shall be under no obligation to accept the lowest or any other offer received in response to this tender (RFP) notice. StockHolding further reserves the right to reject any or all offers based on its own evaluation of the offers received, or on the basis of stability, capabilities, track records, reputation among users and other similar credentials of a System Integrator. When StockHolding makes any such rejection, StockHolding will not be bound to give any reason and/or justification in this regard to the System Integrator.

Annexure – 1
Details of System Integrator's Profile

(To be submitted along with technical bid on Company letter head)

Details filled in this form must be accompanied by sufficient documentary evidence, in order to verify the correctness of the information.

Serial No.	Parameters	Response
1	Name of the Firm/Company	
2	Year of Incorporation in India	
3	Names of the Partners/Directors	
4	Company PAN no	
5	Company GSTN no. (please attach annexures for all states)	
6	Addresses of Firm/Company	
	a) Head Office	
	b) Local Office in Mumbai(if any)	
7	Authorized Contact person	
	a) Name and Designation	
	b) Telephone number	
	c) E-mail ID.	
8	Years of experience in providing Managed Security services for Security Operation Centre (SOC) and link management service	

9	**Financial parameters**		
	Business Results (last three years)	Annual Turnover (Rs. in Crores)	Operating Profit (Rs. in Crores)
	2017-18		
	2018-19		
	2019-20		
	(Only Company figures need to be mentioned not to include group/subsidiary Company figures}	(Mention the above Amount in INR only)	

N.B. Enclose copies of Audited Balance Sheet along with enclosures

Dated this........ Day of 2020
(Signature)
(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the System Integrator

Annexure - 2

Eligibility Criteria (Documents to be submitted online along with Technical Bid)

#	Eligibility Criteria	Compliance (Y/N)	Supporting Evidence
1.	The System Integrator should be in existence for minimum of 15 years as on 31-OCT-2020 and providing Cyber Security services for at least last 10 years.		Certificate of Incorporation
2.	The System Integrator should have the experience of owning and managing a well-established Security Operations Centre (SOC) for at least 10 years. System Integrator shall provide the details of the SOC including the location, infrastructure, tools used, companies served, process and methodology, staff employed.		Self-Declaration from equivalent to Company secretary with Supporting documents should be a SOC related PO dated 13-DEC-2020 or before
3.	The System Integrator should have executed, during any of the last five financial years, at least one SOC contract having value not less than INR 15 Crores OR two SOC contracts having value not less than INR 8 Crores each for any Govt./ BFSI/ PSU/Enterprise organization globally		Self-Declaration from equivalent to Company secretary.

4.	Annual Audited Turnover duringlast three financial years (as per the last published audited balance sheets) should not be less than INR 100 Crores. AND At least INR 35 Crores from InformationSecurity (IS)/ Managed Security Services(MSS) related services and products during any of the last 5 FYs. AND The Net worth of the System Integrator should bepositive CA Certificate with CA's Registration Number/ Seal as per "Specific Requirements". It shall clearly state the'Overall Average Annual Turnover' and 'OverallAverage Annual Turnover From IS/ MSS'.		Self-Declaration from equivalent to Company secretary.
5.	System Integrator's SOC should be ISO 27001 and /or ISO 20000 certified and SOC 2.0 accredited.		Certificates.
6.	The System Integrator should have in minimum 3 BFSI existing customers in India who are using SOC services from the System Integrator for at least last 5 years		Customer references to be provided
7.	System Integrator should be providing NGSOC services to 3 BFSI Customers using proposed SIEM solution which leverages Big Data analytical platform that is capable of detecting anomalies in the network over and above rule/ use case-based technologies can detect.		To provide 3 BFSI clients PO for Next Generation SOC Services
8.	The System Integrator's SOC service should be recognized by leading analyst's like Gartner & Forrester.		Share analyst reports to confirm the same.
9.	The System Integrator must be empaneled with CERT-In as Information Security Audit Organization		Self-Declaration from equivalent to Company secretary
10.	System Integrator should have below mentioned best in class tools/technology & application listed in latest Gartner quadrants report which must be fulfilling the NHB business requirements:· SIEM· Threat Intelligent Feed		Self-Declaration from equivalent to Company secretary

11.	The System Integrator Company should have at-least 100 qualified Information Security / Cyber Security Professionals (DISA/CISA/CISSP/CISM/CDAC/ CEH/ITIL/PMP/ISO 27001/CCSA certified) in their payroll.		Self-Declaration from equivalent to Company secretary
12.	The system Integrator shall not assign or sub-contract the assignment or any part thereof to any other person/firm.		Self-Declaration from equivalent to Company secretary
13.	System Integrator SOC should be owned by them and not outsourced to any third party		Self-Declaration from equivalent to Company secretary

Note:

1 Letter of Authorization shall be issued by either Managing Director having related Power of Attorney issued in his favor or a Director of the Board for submission of Response to RFP

2 All self-certificates shall be duly signed and Stamped by Authorized signatory of the System Integrator Firm unless specified otherwise.

3 *System Integrator e should provide complete response a Yes/ a No answer is not acceptable...*

4 *Details of clients and relevant contact details are mandatory. System Integrators may take necessary approval of the clients in advance before submission of related information. StockHolding will not make any separate request for submission of such information.*

Dated this........ Day of 2020
(Signature)
(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the System Integrator)

Annexure-3
TECHNICAL BID

S.No	Evaluation Parameters / Credentials	Credentials for awarding score (It should be clearly understood that in case of ambiguity or lack of clarity in the documents submitted, the decision of StockHolding is final for awarding the marks against each of the specified items.)
1	System Integrators no. of Years of experience in providing Managed Security Services(MSS) along with Security Operation Centre (SOC) services (As on 31st March 2020)	The marks to be awarded as per the credentials submitted in respect of clients serviced in India: 20 Marks for 15 years and above. 15 Marks for 12 years and above. 10 Marks for 10 years and above. Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.

2	The System Integrator's experience in providing Managed Security Services (MSS) along with Security Operation Centre (SOC) services in India to BFSI/PSUs in India. (As on 31st March 2020)	The marks to be awarded as per the credentials submitted in respect of BFSI/PSUs serviced: 20 Marks for 5 BFSI/PSUs or above. 15 Marks for 4 BFSI/PSUs. 10 Marks for 3 BFSI/PSUs. Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.
3	No. of BFSI/PSUs where the proposed SIEM solution should have been providing SOC services in India during the last three years (As on 31st March 2020)	The marks to be awarded as per the credentials submitted in respect of BFSI/PSUs serviced: 20 Marks for 5 BFSI/PSUs or above. 15 Marks for 4 BFSI/PSUs. 10 Marks for 3 BFSI/PSUs. Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.
4	The System Integrator's inclusion in the Gartner or Forrester reports on Managed Security Services (MSS) or Managed Detection &Response Services (MDR) specifically in past 3 years (2020, 2019 & 2018)	The marks to be awarded as per the credentials submitted in respect of no. of years: 20 marks for inclusion in both Gartner & Forrester. 15 marks for only 1 analyst recognition. 10 marks for only 1-year recognition. Please provide relative document of the Gartner or Forrester reports fulfilling the mentioned criteria.

5	System Integrator having a SoC and DR SOC functional in India for: (Max Marks 10)	More than 4 years --------------- Marks 10 4 years ------------------------------ Marks 05
6	The System Integrator's SOC infrastructure must be ISO certified and must provide SOC -2 audit report.	(System Integrator must provide a copy of valid ISO Certification for the SOC facility and extract of most recent SOC-2 report) (Max Marks 10)

REQUEST FOR PROPOSAL FOR
MANAGED SECURITY SERVICES FOR SECURITY OPERATION CENTRE

Annexure-4
Final No Regret Commercial Bid FORMAT

Commercial for the period MAR 2021 to FEB 2022

S/N.	Line Item	Total Price (Rs.)
1	Security Services for Security Operation centre	

Commercial for the period MAR 2022 to FEB 2023

S/N.	Line Item	Total Price (Rs.)
1	Security Services for Security Operation centre	

Commercial for the period MAR 2023 to FEB 2024

S/N.	Line Item	Total Price (Rs.)
1	Security Services for Security Operation centre	

GRAND TOTAL FOR THE THREE YEARS = INR

In words:

Note:

(1) Applicable GST payable at actual as per prevailing rate as per Government notification. In case of tax exemption or lower TDS; System Integrator has to submit letter from Government Authority for tax exemption or lower TDS (to be submitted along with each of the invoice(s).

(2) System Integrator must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. Unit price must be quoted in word and number. All fields must be filled in correctly. Please note that any Commercial Offer, which is conditional and / or qualified or subjected to suggestions, will also be summarily rejected. This offer shall not contain any deviation in terms & conditions or any specifications, if so such an offer will also be summarily rejected.

Dated this........ Day of 2020
(Signature)
(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the System Integrator)

Annexure - 5

Interest free Earnest Money Deposit (EMD) Format OR MSME/NSIC for Managed security service for security operation centre

PAN & GST number of System Integrator	Bank Name & branch address ,IFSC code	Bank account number	EMD amount paid in INR	UTR No. / MSME/NSIP document no	Date of Payment (NEFT)	Document MSME/NSIC / EMD Bank receipt to be uploaded
1.						

Dated this........ Day of 2020
(Signature)
(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the System Integrator)

REQUEST FOR PROPOSAL FOR
MANAGED SECURITY SERVICES FOR SECURITY OPERATION CENTRE

Annexure - 6

Covering Letter-1

(To be executed on plain paper and submitted only by the successful System Integrator)

(__________________________________ Name of the Department / Office) RFP No: IT-04/2020-21 dated 14-DEC-2020 for______________________________

This pre-bid pre-contract Integrity Pact (Agreement) (hereinafter called the Integrity Pact) (IP) is made on ______ day of the _______________________, between, on one hand, *StockHolding* , a company incorporated under Companies Act, 1956, with its Registered Office at 301, Centre Point Building, Dr. Babasaheb R. Ambedkar Road, Parel, Mumbai – 400012 , acting through its authorized officer, (hereinafter called **Principal**), which expression shall mean and include unless the context otherwise requires, his successors in office and assigns) of the First Part **And**
M/s.____
____ (with complete address and contact details) represented by Shri ____ (i.e. s (System Integrators) hereinafter called the **`Counter Party')** which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

AND WHEREAS the PRINCIPAL/Owner values full compliance with all relevant laws of the land, rules, regulations economic use of resources and of fairness/transparency in its relation with System Integrator(s) /Contractor(s)/Counter Party(ies).

AND WHEREAS, in order to achieve these goals, the Principal/Owner has appointed Independent External Monitors (IEM) to monitor the Tender (RFP) process and the execution of the Contract for compliance with the principles as laid down in this Agreement.

WHEREAS THE Principal proposes to procure the Goods/services and Counter Party is willing to supply/has promised to supply the goods OR to offer/has offered the services and WHEREAS the Counter Party is a private Company/Public Company/Government Undertaking/ Partnership, constituted in accorded with the relevant law in the matter and the Principal is a Government Company performing its functions as a registered Public Limited Company regulated by Securities Exchange Board of India. **NOW THEREFORE**, To avoid all forms of corruption by following a system that is fair, transparent and free from any influence prejudiced dealings prior to, during and subsequent to the tenor of the contract to be entered into with a view to - Enabling the PRINCIPAL to obtain the desired goods/services at competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and Enabling the Counter Party to abstain from bribing or indulging in any type of corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the PRINCIPAL will commit to prevent corruption, in any form, by its officials by following transparent procedures. The parties hereto hereby agree to enter into this Integrity Pact and agree as follows**:**

I. Commitment of the Principal / Buyer

1. The Principal Owner commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

   a) No employee of the Principal/Owner, personally or through any of his/her family members, will in connection with the Tender (RFP) or the execution of the contract, procurement or services/goods, demand, take a promise for or accept for self or third person, any material or immaterial benefit which the person not legally entitled to.

   b) The Principal/Owner will, during the Tender (RFP) Process treat all System Integrator(s)/Counter Party (ies) with equity and reason. The Principal / Owner will, in particular, before and during the Tender (RFP) Process, provide to all System Integrator(s) / Counter Party (ies) the same information and will not provide to any System Integrator(s)/Counter Party(ies) confidential / additional information through which the System Integrator(s)/Counter Party(ies) could obtain an advantage in relation to the Tender (RFP) Process or the Contract execution.

   c) The Principal / Owner shall endeavor to exclude from the Tender (RFP) process any person, whose conduct in the past been of biased nature.

2. If the Principal / Owner obtains information on the conduct of any of its employees which is a criminal offence under the Indian Penal Code (IPC) / Prevention of Corruption Act, 1988 (PC Act) or is in violation of the principles herein mentioned or if there is a substantive suspicion in this regard, the Principal / Owner / *StockHolding* will inform the Chief Vigilance Officer through the Vigilance Officer and in addition can also initiate disciplinary actions as per its internal laid down policies and procedures.

II. Commitments of Counter Parties/System Integrators

1. The Counter Party commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of bid or during any pre-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following. Counter Party (ies) / System Integrators commits himself to observe these principles during participation in the Tender (RFP) Process and during the Contract execution.
2. The Counter Party will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PRINCIPAL, connected directly or indirectly with the bidding process, or to any person organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.
3. The Counter Party further undertakes that it has not given, offered or promised to give directly or indirectly any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Principal / *StockHolding* or otherwise in procurement the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Principal / *StockHolding* for

forbearing to show favor or disfavor to any person in relation to the contract or any other contract with the Principal / *StockHolding*.

4. System Integrator / Counter Party shall disclose the name and address of agents and representatives, if any, handling the procurement / service contract.
5. System Integrator / Counter Party shall disclose the payments to be made by them to agents / brokers; or any other intermediary if any, in connection with the bid / contract.
6. The System Integrator / Counter Party has to further confirm and declare to the Principal / *StockHolding* that the System Integrator / Counter Party is the original integrator and has not engaged any other individual or firm or company, whether Indian or foreign to intercede, facilitate or in any way to recommend to Principal / *StockHolding* or any of its functionaries whether officially or unofficially to the award of the contract to the System Integrator / Counter Party nor has any amount been paid, promised or intended to the be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.
7. The System Integrator / Counter Party has to submit a Declaration along with Technical Bid, as given at Annexure

   6. If bids are invited through a Consultant a Declaration has to be submitted along with the Technical Bids as given at Annexure.
8. The System Integrator / Counter Party, either while presenting the bid or during pre- contract negotiation or before signing the contract shall disclose any payments made, is committed to or intends to make to officials of *StockHolding* /Principal, or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.
9. The System Integrator / Counter Party will not collude with other parties interested in the contract to impair the transparency, fairness and progress of bidding process, bid evaluation, contracting and implementation of the Contract.
10. The System Integrator / Counter Party shall not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
11. The System Integrator shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the Principal / *StockHolding* as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The System Integrator / Counter Party also Undertakes to exercise due and adequate care lest any such information is divulged.
12. The System Integrator / Counter Party commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
13. The System Integrator / Counter Party shall not instigate or cause to instigate any third person including their competitor(s) of bidding to commit any of the actions mentioned above.
14. If the System Integrator / Counter Party or any employee of the System Integrator or any person acting on behalf of the System Integrator / Counter Party, either directly or indirectly, is a relative of any of

the official / employee of Principal / *StockHolding*, or alternatively, if any relative of an official / employee of Principal /

StockHolding has financial interest / stake in the System Integrator's / Counter Party firm, the same shall be disclosed by the System Integrator / Counter Party at the time of filing of tender (RFP).

15. The term `relative‟ for this purpose would be as defined in Section 2 Sub Section 77 of the Companies Act, 2013.
16. The System Integrator / Counter Party shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employees / officials of the Principal / *StockHolding*
17. The System Integrator / Counter Party declares that no previous transgression occurred in the last three years immediately before signing of this IP, with any other Company / Firm/ PSU/ Departments in respect of any corrupt practices envisaged hereunder that could justify System Integrator / Counter Party exclusion from the Tender (RFP) Process.
18. The System Integrator / Counter Party agrees that if it makes incorrect statement on this subject, System Integrator / Counter Party can be disqualified from the tender (RFP) process or the contract, if already awarded, can be terminated for such reason.

III. Disqualification from Tender (RFP) Process and exclusion from Future Contracts

1. If the System Integrator(s) / Contractor(s), either before award or during execution of Contract has committed a transgression through a violation of Article II above or in any other form, such as to put his reliability or credibility in question, the Principal / *StockHolding* is entitled to disqualify the System Integrator / Counter Party / Contractor from the Tender (RFP) Process or terminate the Contract, if already executed or exclude the System Integrator / Counter Party / Contractor from future contract award processes. The imposition and duration of the exclusion will be determined by the severity of transgression and determined by Principal / *StockHolding*. Such exclusion may be for a period of 1 year to 3 years as per the procedure prescribed in guidelines of the Principal / *StockHolding*.
2. The System Integrator / Contractor / Counter Party accepts and undertake to respect and uphold the Principal / *StockHolding*'s absolute right to resort to and impose such exclusion.
3. Apart from the above, the Principal / *StockHolding* may take action for banning of business dealings / holiday listing of the System Integrator / Counter Party / Contractor as deemed fit by the Principal / Owner / *StockHolding*.
4. The System Integrator / Contractor / Counter Party can prove that it has resorted / recouped the damage caused and has installed a suitable corruption prevention system, the Principal / Owner/ *StockHolding* may at its own discretion, as per laid down organizational procedure, revoke the exclusion prematurely.

IV. Consequences of Breach Without prejudice to any rights that may be available to the Principal / *StockHolding* / Owner under Law or the Contract or its established policies and laid down procedure, the

Principal / *StockHolding* / Owner shall have the following rights in case of breach of this Integrity Pact by the System Integrator / Contractor(s) / Counter Party: -

1. Forfeiture of EMD / Security Deposit : If the Principal / *StockHolding* / Owner has disqualified the System Integrator(s)/Counter Party(ies) from the Tender (RFP) Process prior to the award of the Contract or terminated the Contract or has accrued the right to terminate the Contract according the Article III, the Principal / *StockHolding* / Owner apart from exercising any legal rights that may have accrued to the Principal / *StockHolding* / Owner, may in its considered opinion forfeit the Earnest Money Deposit / Bid Security amount of the System Integrator / Contractor / Counter Party.
2. Criminal Liability: If the Principal / Owner / *StockHolding* obtains knowledge of conduct of a System Integrator / Counter Party / Contractor, or of an employee of a representative or an associate of a System Integrator / Counter

   Party / Contractor which constitute corruption within the meaning of PC Act, or if the Principal / Owner / *StockHolding* has substantive suspicion in this regard, the Principal / *StockHolding* / Owner will inform the same to the Chief Vigilance Officer through the Vigilance Officer.

V. Equal Treatment of all System Integrators/Contractors / Subcontractors / Counter Parties

1. The System Integrator(s) / Contractor(s) / Counter Party (ies) undertake (s) to demand from all subcontractors a commitment in conformity with this Integrity Pact. The System Integrator / Contractor / Counter-Party shall be responsible for any violation(s) of the principles laid down in this Agreement / Pact by any of its subcontractors / sub-s.
2. The Principal / *StockHolding* / Owner will enter into Pacts on identical terms as this one with all System Integrators / Counterparties and Contractors.
3. The Principal / *StockHolding* / Owner will disqualify System Integrators / Counter Parties / Contractors who do not submit, the duly signed Pact, between the Principal / Owner / *StockHolding* and the System Integrator/Counter Parties, along with the Tender (RFP) or violate its provisions at any stage of the Tender (RFP) process, from the Tender (RFP) process.

VI. Independent External Monitor (IEM)

1. The Principal / Owner / *StockHolding* has appointed competent and credible Independent External Monitor (s) (IEM) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Integrity Pact.
2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Chief Executive Officer and Managing Director, Stock Holding Corporation of India Limited
3. The System Integrator(s)/Contractor(s) / Counter Party(ies) accepts that the IEM has the right to access without restriction, to all Tender (RFP) documentation related papers / files of the Principal / *StockHolding* / Owner including that provided by the Contractor(s) / System Integrator / Counter Party. The Counter Party / System Integrator / Contractor will also grant the IEM, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his or any of his Sub-

Contractor's Tender (RFP) Documentation / papers / files. The IEM is under contractual obligation to treat the information and documents of the System Integrator(s) / Contractor(s) / Sub-Contractors / Counter Party (ies) with confidentiality.

4. In case of tender (RFP)s having value of 5 crore or more, the Principal / *StockHolding* / Owner will provide the IEM sufficient information about all the meetings among the parties related to the Contract/Tender (RFP) and shall keep the IEM apprised of all the developments in the Tender (RFP) Process.
5. As soon the IEM notices, or believes to notice, a violation of this Pact, he will so inform the Management of the Principal / Owner /*StockHolding* and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit non-binding recommendations. Beyond this, the IEM has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The IEM will submit a written report to the CEO&MD, *StockHolding*. Within 6 to 8 weeks from the date of reference or intimation to him by the Principal / Owner / *StockHolding* and should the occasion arise, submit proposals for correcting problematic situations.
7. If the IEM has reported to the CEO&MD, *StockHolding* Ltd. a substantiated suspicion of an offence under the relevant IPC/PC Act, and the CEO & MD, *StockHolding* has not within reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the IEM may also transmit the information directly to the Central Vigilance Officer. 8. The word `IEM‟ would include both singular and plural.

VII. Duration of the Integrity Pact (IP)

This IP begins when both the parties have legally signed it. It expires for the Counter Party / Contractor / System Integrator, 12 months after the completion of work under the Contract, or till continuation of defect liability period, whichever is more and for all other System Integrators, till the Contract has been awarded. If any claim is made / lodged during the time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by the CEO&MD *StockHolding*

VIII. Other Provisions

1. This IP is subject to Indian Law, place of performance and jurisdiction is the Head Office / Regional Offices of StockHolding /Principal / Owner who has floated the Tender (RFP).
2. Changes and supplements in any Procurement / Services Contract / Tender (RFP) need to be made in writing. Change and supplement in IP need to be made in writing.
3. If the Contractor is a partnership or a consortium, this IP must be signed by all the partners and consortium members. In case of a Company, the IP must be signed by a representative duly authorized by Board resolution.
4. Should one or several provisions of this IP turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

5. Any dispute or difference arising between the parties with regard to the terms of this Agreement / Pact, any action taken by the Principal / Owner / *StockHolding* in accordance with this Agreement / Pact or interpretation thereof shall not be subject to arbitration.

IX. Legal and Prior Rights

All rights and remedies of the parties hereto shall be in addition to all the other legal rights and remedies belonging to such parties under the Contract and / or law and the same shall be deemed to be cumulative and not alternative to such legal rights and remedies aforesaid. For the sake of brevity, both the Parties agrees that this Pact will have precedence over the Tender (RFP) / Contract documents with regard to any of the provisions covered under this Integrity Pact.

IN WITNESS WHEREOF the parties have signed and executed this Integrity Pact (IP) at the place and date first above mentioned in the presence of the following witnesses: -

----

(For and on behalf of Principal / Owner / *StockHolding*

(For and on behalf of System Integrator / Counter Party / Contractor)

WITNESSES:

1.____ (Signature, name and address)
2.____ (Signature, name and address)
Note: In case of Purchase Orders wherein formal agreements are not signed references to witnesses may be deleted from the past part of the Agreement.

Annexure - 7

Covering Letter on System Integrator's letterhead (Annexure of Integrity Pact)

Date:

To,

--- ---

Sub**:** RFP No: **IT-04/2020-21 dated 14-DEC-2020** for managed security services for security operation centre

Dear Sir,

DECLARATION

Stock Holding Corporation of India Limited (*StockHolding*) hereby declares that *StockHolding* has adopted Integrity Pact (IP) Program as advised by Central Vigilance Commission vide its Letter No. ------------------ Dated --------------- and stands committed to following the principles of transparency, equity and competitiveness in public procurement. The subject Notice Inviting Tender (RFP) (NIT) is an invitation to offer made on the condition that the System Integrator will sign the Integrity Agreement, which is an integral part of tender (RFP) documents, failing which the tenderer / System Integrator will stand disqualified from the tender (RFP) ing process and the bid of the System Integrator would be summarily rejected. This Declaration shall form part and parcel of the Integrity Agreement and signing of the same shall be deemed as acceptance and signing of the Integrity Agreement on behalf of *StockHolding*

Yours faithfully,
For and on behalf of Stock Holding Corporation of India Limited (Authorized
Signatory)

REQUEST FOR PROPOSAL FOR
MANAGED SECURITY SERVICES FOR SECURITY OPERATION CENTRE

Annexure - 8

Compliance Statement

(To be submitted along with Technical bid)

Subject: RFP for Managed security services for security operation centre

Ref: RFP **No: IT-04/2020-21 dated 14-DEC-2020**

DECLARATION

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by StockHolding. We also agree that *StockHolding* reserves its right to reject the bid, if the bid is not submitted in proper format as per RFP.

Sr. No.	Item / Clause of the RFP	Confirmed and Accepted by System Integrator (Yes / No)
1	Eligibility Criteria	
2	Service Level Agreement (SLA) / Scope of Work /Penalty	
3	Non-Disclosure Agreement	
4	Payment Terms	
5	Bid Validity, Order Cancellation, Exit Clause	
6	StockHolding's Right to alter RFP	
7	No Commitment from StockHolding to Accept Lowest or Any Other Bid (RFP)	
8	Force Majeure	
9	Integrity Pact	
10	All General & Other Terms & Conditions in the RFP	
11	Requirement with terms and conditions	
12	Bid Formats (Technical & Indicative Price Bid)	
13	Annexures in the RFP	

Dated this........ Day of 2020
(Signature)
(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the System Integrator)

REQUEST FOR PROPOSAL FOR
MANAGED SECURITY SERVICES FOR SECURITY OPERATION CENTRE

Annexure - 9
Letter of Acceptance
(To be submitted along with Technical Bid)

To,
Stock Holding Corporation of India Limited
SHCIL House, Plot No. P-51, T.T.C. Industrial Area,
M.I.D.C., Mahape, Kalyan-Shil Road,
Navi Mumbai, PIN 400710.

Dear Sir,
Sub**:** RFP no: **IT-04/2020-21 dated 14-DEC-2020** for managed security services for security operation centre

With reference to the above RFP, having examined and understood the instructions, annexures, terms and conditions forming part of the RFP.

We further confirm that the offer is in conformity with the terms and conditions as mentioned in the RFP. We also confirm that the offer shall remain valid for the entire Agreement Period from the date of the offer.

We also understand and accept that StockHolding can modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. We further understand and accept that *StockHolding*'s decision in this regard will be final and binding on us.

We also accept that *StockHolding*'s decisions with reference to this RFP pertaining to evaluation process of System Integrator responses will be final and binding on us. We also understand and accept that no queries will be entertained in this regard by *StockHolding*.

StockHolding is not bound to accept the lowest or any bid received by *StockHolding*, and it may reject all or any bid. If our bid is accepted, we are responsible for the due performance of the contract.

Dated this........ Day of 2020
(Signature)
(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the System Integrator)