Stock Holding Corporation of India Limited

(StockHolding)

RFP Reference Number: CPCM-03/2026-27

Date: 09-Apr-2026

GEM Reference No. - GEM/2026/B/7427591

REQUEST FOR PROPOSAL FOR SELECTION OF SERVICE PROVIDER FOR IMPLEMENTATION & SUPPORT FOR SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) PLATFORM AND MANAGED DETECTION & RESPONSE SERVICES (MDR)

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or information provided subsequently to bidder(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 bidder(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 ("bidders"). The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this 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.

RFP Document Details

Sr. No.	Description	Remarks
1	Name of Organization	Stock Holding Corporation of India Limited
2	RFP Reference Number	CPCM-03/2026-27
3	Requirement	Request for proposal (RFP) for selection of Service Provider for implementation & support SIEM (Security Information and Event Management) Platform and Managed Detection & Response Services (MDR)
4	Interest free Earnest Money Deposit (EMD) [*]	Rs.22,50,000/- (Indian Rupees Twenty Two Lakhs Fifty Thousand only) 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/BG/FDR on StockHolding's Bank Account No.: 004103000033442 Bank: IDBI Bank (Nariman Point Branch) IFSC: IBKL0000004. Please share the UTR details to us on below mentioned email address. Bidders registered under Micro & Small Enterprises (MSE) for specific trade are exempted from EMD. Bidders shall upload the scanned copy of necessary documents as part of eligibility criteria documents.
5	Email Id for queries up to Pre-Bid Meet	CPCM@stockholding.com
6	Date of Issue of RFP Document	09-Apr-2026
7	Date, Time and place for online Pre-bid meeting	15-Apr-2026 03:00 PM For participation in pre-bid meeting, please send mail for online meeting link to CPCM@stockholding.com before 15-Apr-2026 12:00 PM
8	Last date for submission of pre-bid queries	15-Apr-2026 All responses to pre-bid queries will be published on the website. Any queries submitted after the specified deadline will not be considered.
9	Last Date for Submission of Online Bid	24-Apr-2026 11:00 AM

10	Date of opening bid	24-Apr-2026 11:30 AM

This bid document is not transferable.

StockHolding reserves the right to modify/update activities/ dates as per requirements of the process.

Table of Contents

SUBMISSION OF PROPOSAL

StockHolding invites e-tender through GeM Portal, in two bid system (Technical and Commercial bid), from firm/company who has proven experience in implementation and support for SIEM (Security Information and Event Management) Platform and Managed Detection and Response Services (MDR).

Submission of Bids:

The online bids will have to be submitted within the time specified on website https://gem.gov.in/ the following manner:-

1. Technical Bid (.pdf files)
2. Commercial Bid (.pdf files)

Invitation for bids:

This "Invitation for bid" is meant for the exclusive purpose of "implementation and support for SIEM (Security Information and Event Management) Platform and Managed Detection and Response Services (MDR)" for StockHolding as per the terms, conditions, and specifications indicated in this RFP and shall not be transferred, reproduced or otherwise used for purposes other than for which it is specifically issued.

Objective of this RFP

The objective of this RFP is to appoint Service Provider to provide, implement and support for SIEM (Security Information and Event Management) Platform and Managed Detection and Response Services (MDR) so as to comply with the circulars and advisories issued by CERT-in, NCIIPC, SEBI, NSDL, CDSL, PFRDA, IRDA, RBI etc. 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.

Due Diligence:

The bidder 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 bidder'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 bidder 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 Bidder Details – Annexure 1
b Requirement with Scope of Service and Terms and Conditions
c Format for Eligibility Criteria - Annexure 2
d Technical Bid – Annexure 3
e Format for Commercial Bid - Annexure 4
f Integrity Pact (Text) - Annexure 5
g Compliance Statement - Annexure 6
h Format for bank Guarantee – Annexure 7
i Format for Non-disclosure Agreement - Annexure 8

Clarifications regarding RFP Document:

a Before bidding, the bidders 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.
b A bidder requiring any clarification for their queries on this RFP may be obtained via email to CPCM@StockHolding.com
c StockHolding shall not be responsible for any external agency delays.
d StockHolding reserves the sole right for carrying out any amendments / modifications / changes in the bidding process including any addendum to this entire RFP
e 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 bidders, modify this RFP Document.
f StockHolding reserves the rights to extend the deadline for the submission of bids, if required. However, no request from the bidders for extending the deadline for submission of bids, shall be binding on StockHolding.
g StockHolding reserves the right to amend / cancel / postpone / pre-pone the RFP without assigning any reasons.
h It may be noted that notice regarding corrigendum/addendums/amendments/response to bidder's queries etc., will be published on StockHolding's website only. Prospective bidders shall regularly visit StockHolding's same website for any changes/development in relation to this RFP.
i It may be noted that bidder mentioned in the document may be either OEM/Distributor/System Integrator (SI).

Validity of offer:

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

ELIGIBILITY CRITERIA (Documents to be Submitted Online)

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 invitation to bid is open to all bidders who need to qualify the eligibility criteria as given below. Eligibility criteria are mandatory and any deviation in the same will attract bid disqualification.

Guidelines to be followed prior to submitting an application-

Bidder should upload all supporting documents at the time of submission duly signed and stamped on their company's letter head.

SI. No	Criteria	Documents to be submitted by Bidder
1	The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of SIEM and MDR services implementation and support for the period of 7 years.	Copy of Certificate of Incorporation issued by the Registrar of Companies and Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory along with supporting documents for SOC related PO on or before RFP Date
2	The bidder should have an average annual turnover of at least Rs. 6 Crores per annum for last 03 (three) financial years (i.e. 2022-23, 2023-24 and 2024-25). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last three financial years.
3	The Bidder should have Positive Net worth minimum Rs. 2 crores for each of the last 03 (three) audited financial years (i.e. 2022-23, 2023-24 and 2024-25)	Certificate from CA mentioning networth for the past three financial years.
4	The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution. Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP.	Copy of Purchase Order /Completion certificate with Customer Name and Address, Contact Person, Telephone Nos. Fax and e-mail Address and customer reference to be provided

5	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 3 years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
6	The bidder must possess at the time of bidding, following valid certifications: ISO 9001:2008 or latest/ISO 20000 or ISO 27001:2013 or latest	Relevant valid ISO Certificates
7	The bidder must have a direct partnership with the supplier of the SIEM tool. One Service Provider can bid only with one OEM as regards SIEM solution is concerned	MAF from OEM to be submitted
8	Bidder should have Support office at MMRDA Region or Pune.	Bidder to provide office address along with GST details.
9	The Bidder to submit signed & stamped Integrity Pact as per Annexure - 5	Self-declaration by authorized signatory of Bidder

BIDS PREPARATION AND SUBMISSION DETAILS

The online bids will have to be submitted within the time specified on website https://gem.gov.in/ . Bidders must familiarize (if not already) with the Portal and check/ fulfil the pre-requisites to access and submit the bid there.

1. Submission of Bids

a) The required documents for Eligibility Criteria, Commercial Bid must be submitted (uploaded) online on GeM portal. Eligibility Criteria and Commercial Bid should be complete in all respects and contain all information asked for in this RFP document
b) The offer should be valid for a period of at least **90 days** from the date of submission of bid.
c) The Bidder shall fulfil all statutory requirements as described by the law and Government notices. The Bidder 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 bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP document(s). Failure to furnish all information required as mentioned in the RFP document(s) or submission of a proposal not substantially responsive to the RFP document(s) in every respect will be at the bidder's risk and may result in rejection of the proposal.
e) Delayed and/or incomplete bid shall not be considered.
f) There may not be any extension(s) to the last date of online submission of Eligibility Criteria details and commercial Price bids. This will be at the sole discretion of StockHolding.

2. Evaluation of Bids

StockHolding will evaluate the bid submitted by the bidders under this RFP. The eligibility bid submitted by the Bidder will be evaluated against the Eligibility criteria set forth in the RFP. The Bidder needs to comply with all the eligibility criteria mentioned in the RFP to be evaluated for evaluation. Noncompliance to any of the mentioned criteria would result in outright rejection of the bidder's proposal. The decision of *StockHolding* would be final and binding on all the bidders to this document.

StockHolding may accept or reject an offer without assigning any reason what so ever. The bidder is required to comply with the requirement mentioned in the RFP. Non-compliance to this may lead to disqualification of a bidder, which would be at the discretion of *StockHolding*.

a) Please note that all the information desired needs to be provided. Incomplete information may lead to non-consideration of the proposal.
b) The information provided by the bidders in response to this RFP document will become the property of StockHolding.

Evaluation Process

First the 'Eligibility Criteria bid document' will be evaluated and only those bidders who qualify the requirements will be eligible for 'Technical bid'. In the second stage, for only those bidders who meets the 'Eligibility Criteria', technical bids will be evaluated, and a technical score would be arrived at. In third stage, only those bidders, who have qualified in the technical evaluation, shall be invited for commercial evaluation.

Eligibility Criteria Evaluation

The bidder meeting the Eligibility Criteria as per **Annexure 2** will be considered for Technical evaluation. Any credential/supporting detail mentioned in "Annexure 2 – Eligibility Criteria" and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

Technical Bid Evaluation

The Technical bids of only those bidders shall be evaluated who have satisfied the eligibility criteria bid. *StockHolding* may seek clarifications from the any or each bidder as a part of technical evaluation requirements as mentioned in Annexure 3. All clarifications received by within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the *StockHolding*.

The proposal submitted by the bidders shall, therefore, be evaluated on the following criteria:

Sl. No	Parameter	Scores	Max Scores
A. **BASED ON VENDOR TURNOVER & EXPERIENCE (70 MARKS)**			
1	Average annual turnover of the bidder during last 03 (three) years (i.e. 2022-23, 2023-24 and 2024-25)	• 6 Crores >= 10 Crores : 10 Marks • >10 Crore but <= INR 15 Crore : 12 Marks • More than INR 15 crore : 15 Marks	15
2	Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution each during last 05 (five) years in India	• 1-3 Projects – 10 Marks • 4-5 Projects – 12 Marks • More than 5 Projects – 15 Marks	15

	Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP.		
3	Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India	• 1-3 Projects – 5 Marks • 4-5 Projects – 7 Marks • More than 5 Projects – 10 Marks	10
4	OEM solution must be positioned in the respective Leader's quadrant/category of the latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave reports for proposed SIEM Solution	Presence of OEM Solution in Leader's quadrant/category – 10 Marks	10
5	The bidder should have minimum three (3) resources certified/ trained on the proposed SIEM solution.	The bidder must submit relevant certifications or details of the trained resources. Evaluation will be based on the number of certified/trained resources provided, as follows: 3 resources – 4 Marks 4 to 5 resources – 6 Marks More than 5 resources – 8 Marks	8
6	Customer reference for proposed SIEM-MDR Solution during the last 5 years as on RFP date	3 Customer reference Feedback from existing customer 2 = Average, 3 = Good, 4 = Excellent	12
B. **TECHNICAL PRESENTATION (30 MARKS)**			
7	Bidder's technical presentation	• Understanding of the Project requirements – 5 marks • OEM/Bidder's SIEM and MDR Implementation Capabilities – 5 marks • Relevant Experience in managing SIEM and MDR Solution – 5 marks • Proposed SIEM and MDR Features - 10 marks • Approach and Methodology of solution implementation and SLA management – 5 marks	30

Note:

- The bidder is required to provide documentary evidence for each of the above criteria.

- StockHolding shall verify the credentials submitted with the respective issuer and understand the credentials claimed for the purpose of evaluation and awarding marks.
- The bidder to submit appropriate credentials [other than self- certification] in respect of each of the item.
- Technical proposals will be evaluated based on the total marks obtained across all technical evaluation criteria. Only those bidders who achieve a minimum cumulative score of 60 marks in the technical evaluation will qualify for the commercial bid evaluation.

Commercial Bid Evaluation

Selection of bidders for commercial evaluation stage -

Only those bidders who achieve a minimum cumulative score of 60 marks in the technical evaluation

L1 bidder will be selected based on the lowest quote submitted.

REQUIREMENT

Stockholding inviting bids from firm/company/organization who has proven experience implementation and support for SIEM (Security Information and Event Management) Platform and Managed Detection and Response Services (MDR).

Scope of Work (SOW)

StockHolding Corporation of India Limited (StockHolding) is floating a request for proposal for MSSP (Managed Security Service Provider) to provide managed security services (MSS) / Security Operation Centre (SoC) Operations management from Stockholding's Data Centre locations. Over the years, StockHolding has been scaling up as well as planning to scale up its cyber defense by deploying various technological controls like Cloud based Security Information and Event Management (SIEM), Managed Detection and Response (MDR) Services, Web Site Scanning Suite (WSS), Anti-phishing, Brand Monitoring and Brand Protection, Deep and Dark Web Monitoring, Next Generation (NGX) Firewalls, Intrusion Prevention System (IPS), Virtual Private Networks (VPN), Distributed Denial of Service (DDOS) Mitigation, Web Application Firewall (WAF), Hybrid Proxy Management, Endpoint Detection and Response (EDR), Data Leakage Protection (DLP), Application Delivery Controller (ADC), Management and maintenance of Secure Active Directory and Patch Management SCCM onsite setup and so on.

Considering all these factors, StockHolding has included a detailed scope of work in the request for proposal (RFP) for SIEM-MDR services to be provided for StockHolding for a period of 03 (three) years.

Security Information and Event Management:

The SIEM solution is required to collect logs from network devices, servers, application security logs, Anti-virus, Security devices, Security solutions like VA tool etc. In addition, the logs being generated by the solutions deployed as part of the SOC implementation need to be collected by the SIEM. The Service Provider should perform the following as part of the SIEM.

Expectation from Managed Detection and Response (MDR) Services:

High Speed Threat Detection and Response: AI platform and threat hunters continuously scan our entire IT stack for threats and deliver high speed defence for us. Early detection capabilities clubbed with speedier response helps pre-empt and combat known and unknown threats proactively.

No Half-Measures in Defending the Cyber Assets: MDR offering to provide for all six components of threat management – intelligence, analytics, SIEM, forensics, cyber incident remediation, and breach management—to protect StockHolding's critical infrastructure and networks.

Low Noise, High Touch Service: Traditional SIEM-based security monitoring cannot detect complex, targeted, or unknown attacks. It is unable to analyse a high volume of varied data. In short: it is unable to defend StockHolding from next-generation cyber-attacks. Security

professional along with AI platform, can provide validated threats and high touch response services, to StockHolding.

Solution Implementation

a) SIEM solution shall be implemented in Service Provider's Data Centre or Cloud based. The Service Provider shall ensure that Data Centre / Cloud Service shall be hosted in India and in no circumstances data shall not move out of India during the entire contract duration.
b) Service Provider's MDR Team shall be based offshore – out of Service Provider's offices.
c) Implement the SIEM tool to collect logs from the identified devices / applications / databases etc.
d) Provide and/or develop parsing rules for standard/ non-standard logs respectively.
e) Implement correlation rules based on out-of-box functionality of the SIEM solution and also based on the use-cases identified.
f) Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool.
g) Build custom interfaces/ Connector for Applications. To begin with StockHolding will start with integration of critical applications. Service Provider can be asked for integrating further more applications if found critical and required by StockHolding.
h) While, it is expected that connectors for all the standard applications and devices will be readily available with the Service Provider and connector for mostly in-house/custom built applications will need to be developed. Service Provider is be expected to develop connector for the custom built applications specifically developed for StockHolding.
i) The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by StockHolding as per the SOW including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations i.e. DC, DR and branch offices, etc.
j) The solution should be able to handle at least 2000 sustainable EPS and scalable to 5000 Peak EPS.
k) The MDR team shall coordinate with StockHolding's SOC Team to on-board and integrate as per the requirement of devices on boarded with MDR.
l) Selected Bidder will customize incident management / dashboard / reports for StockHolding and will modify the same as per the changing requirement of StockHolding.
m) Bidder will also supply all the necessary hardware, software and supporting accessories etc. for integration of the components supplied for CSOC. REC will supply only the Rack space, power and network points.
n) The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days

Log Collection

Logs from all the in-scope devices and additional devices integrated as part of contract period located at the geographically dispersed location should be collected. Bidder / Vendor should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. The log baseline should be in line with industry best practices. In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer. Only in case where remote log collection is not feasible, bidder / vendor should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement. Prepare Daily, Weekly, Monthly compliance reports.

Log Correlation

Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by the bidder on regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents.

Alert Generation

Solution should be capable to generate alerts, register and send/receive the same through message formats like SMTP, SMS, Syslog, and SNMP as per user configurable parameters.

Event viewer / dashboard / reports / incident management

SIEM Solution should provide web-based facility to view security events and security posture of the StockHolding's Network and register incidents. Solution should have drill down capability to view deep inside the attack and analyze the attack pattern. Dash board should have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc. Dashboard should have Role based as well as Discretionary access control facility to restrict access to incidents based on user security clearance level. Solution should provide various reports based on user configurable parameters and standard compliance reports like ISO27001, IT Act and regulatory reports. Selected bidder will customize incident management / dashboard / reports for StockHolding and will modify the same as per the changing requirement of StockHolding.

Incident Management Tool

a) The principal goal of the incident management process is to identify anomalous activities in the environment, contain those events and restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus facilitating continued service quality and availability.
b) Solution should be able to register any security event and generate trouble ticket.

c) Solution should provide complete life cycle management (work flow) of trouble tickets from incident generation till closure of the incident.
d) Bidder should also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate/remediate, recover and learn from the incidents responded to.
e) Solution should provide the logging facility to different levels of users to monitor and manage the incidents generated for closure of the same as per the defined workflow.
f) Solution should be able to integrate with different tools such as SIEM tool, Vulnerability Management tool etc. Incident management should include escalation as per the escalation matrix. However, it is preferred that the SIEM should have an inbuilt integrated incident management tool.
g) Notifications - The Notification Matrix defines the Stockholding's contacts, the incident management process step (initial, diagnose, update and resolve), the method (telephone, mobile, SMS, email) and hours (business hours or after hours). The Notification Matrix shall be customizable as per configuration item.
h) Develop workflow for incident management tool and be responsible for end to end incident management lifecycle.

Managed Detection and Response Services

a) 24x7 monitoring of security alerts (from SIEM), prioritizing and notifying high priority alerts.
b) Provide Assistance for StockHolding's compliance needs- like ISO 27001:2022 or latest, SOC2 Type 2 Audits etc. and internal policy violations in standard formats.
c) Investigation on potential incidents and high priority alerts.
d) Raising remediation tickets to pre-defined users with recommendations and/or response playbooks
e) 24x7 access to security operations personnel over email, voice and video calls and chats.
f) Publishing Monthly MIS report based on predefined dashboards and reports.
g) Curating threat intelligence (TI) relevant for our organization and notifying on threats matching such TI.

Brief description of how operations are performed post Implementation

a) Security Monitoring: Service Provider starts the MDR Remote Log Monitoring service upon successful implementation of technology/platform. The alerts generated on Alerting Sources (SIEM, RCE, IPS, EAF, etc.) are fed in to MDR platform and investigated for who, what, when, and how to determine extent of the impact.
b) Service Provider's MDR offering validates the threats and provides deep incident analysis combining their platform with specialized incident responders. As part of the service, triaging of alerts begin to focus on the most relevant threats and then investigates them to establish if there is a security incident. All the relevant evidences and artefacts related to investigation are stored and maintained in the platform. Alerts

are converted into more significant information such as the attack chain, blast radius, and potential impact to assets.

c) Threat Anticipation: This is threat intelligence in action, and tailored threat anticipation goes far beyond traditional passive threat intelligence feeds available. Global threat intelligence is applied in StockHolding's specific context to enhance our protection. A key part of the MDR service from Service Provider is to gather data and intelligence on threats and attacks worldwide, and to then distil the information to identify which customers might be affected. Service Provider's Threat Anticipation Service is designed to help us stay protected from the latest threat and vulnerabilities by providing actionable inputs related to Vulnerability, Threat and Threat Intel. The TA feed is sent from Service Provider's Intel. Threat Intelligence component of TA feed is fed directly into the MDR platform and is tracked and closed for implementation delivering Actionable Threat Anticipation i.e. From Security News to Protection within Hours.

d) Auto Containment: Service Provider's auto remediation to quickly contain threats by enabling rules on firewall, NGFW, IPS, Proxy, EDR, WAF, Patch management, Routers or AD. Service Provider will integrate our security devices and push rules based on pre-defined response playbooks, for us. Incase auto-remediation is not possible, Service Provider to coordinate with StockHolding's SOC Team to manually apply the changes.

e) Threat Hunting: Threat hunting advocates – "Don't wait for alerts to show up; hunt them". Output of advanced security analytics models run on the platform which is analyzed by a specialized hunting team and the data is queried further to detect threats that may have bypassed other security controls or use cases. This is security analytics in action: MSSP should apply data science and machine learning models to network, application, user, and machine data to proactively hunt for unknown and hidden threats in our environment.

f) As a part of the Standard MDR offering, Service Provider should detect, investigate and contain threats. Post that, they will send out tickets to StockHolding's SOC team for mitigation and response actions within our network. They will also provide playbooks and knowledge base to help us resolve these tickets. StockHolding's SOC team can reach back to them for query resolution but such support is provided on best effort basis.

Security solutions to be integrated with SIEM Platform

Security solutions to be integrated with SIEM, but not limited to the below list. The below inventory could change depending upon installation of new systems and components based on StockHolding's requirements, during the course of the period of assignment. The Service Provider chosen shall, however, undertake to support / such new additions to the infrastructure also at no additional cost to StockHolding.

Sr. No.	Key Solutions
1	WAF Web Application Firewall

2	NAC Network Access Control
3	Perimeter Firewall and Intrusion Prevention System (IPS)
4	Brand Protection and Monitoring Logs, Website Monitoring Service against Defacement
5	Anti-Phishing Service Logs
6	Packet Analysis
7	Database and Compute Server Audit Logs
8	End Point Protection
9	Active Directory Logs
10	Oracle NSG and VMWare NSX Logs
11	Application Delivery Controller (ADC) Logs
12	PIM, PAM, CISCO ISE Logs, CISCO ESA logs,
13	Routers and Switches
14	Proxy
15	Oracle Exadata and PCA
16	VMware Private Cloud

Deliverables

Managed Detection and Response Sizing and Capabilities

Project Initiation and Transition: As a part of the project initiation phase, Service Provider's program manager will conduct a Kickoff meeting and provide walkthrough of scope, pre-requisites, implementation plan, task management tool, escalation Matrix and Governance Model.

Service Provider will provide and follow an agile approach for Integration of log sources. Their methodology is described below:

- Critical First - Critical log sources are monitored first. This will reduce the risk of breach.
- Incremental Value – Phase wise approach will ensure StockHolding see incremental value.
- Continuous Improvements – Learnings from every phase can be deployed in the latter phases.
- Quick value realization – StockHolding will be able to see the value of the service at high speed and not wait for all log sources.

Service Provider will deliver:

- Unified Tool - One click access to program Status. Access and demo will be provided during the pre-kick off discussion.
- Accountability - All tasks of the project are assigned on Service Provider's tool with a due date. The Managed Service team and MDR tasks are assigned on the tool.

- Dashboard - Risks, dependencies, milestones, and work progress can be viewed in a single click – anytime and anywhere transparency

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 Service Provider 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. Service Provider 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, Service Provider 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, Service Provider 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. Existing Raw logs should also be accessible in SIEM platform, additionally collectors to be made available as per stockholding list of Devices and use cases.

Logging of Critical Devices

a) The Service Provider is required to maintain the syslog of the devices installed at DC, DR and NDR locations for a period of 180 days.
b) The logs will be reviewed by StockHolding officials on quarterly and half yearly basis and same has to be ensured by Service Provider.
c) Service Provider will design and implement all simple scripts that may be needed to analyse logs and produce reports as required by StockHolding officials.

Logging of Critical Devices

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. 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 a 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 180 days log data should be available online. Service Provider 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. Service Provider will coordinate with StockHolding SOC 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. Service Provider has to ensure that all such alert mechanisms are intact and brought to the notice of StockHolding 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. Service Provider's team should analyse the logs on regular basis and drill down MDR's capability to view deep inside the attack and analyse the attack pattern. Dash board shall 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 latest regulatory reports. Service Provider has to ensure that StockHolding should get all the configured reports to ensure compliance.

Service Provider 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 Service Provider.

Integration with in-scope monitored devices

Service Provider's 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.

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.

Workflow Automation

Service Provider 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

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

Periodic Review of the project

StockHolding officials will hold a meeting with the senior officials of 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.

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

Transition Management (On-boarding and During-Exit)

StockHolding 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 Service Provider. StockHolding has considered a transition period of 3 months from existing Service Provider to new Service Provider for smooth transfer of the SOC services handover process.

Service Provider 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.

Service Provider will be responsible for planning, preparing and submitting a Transition Plan to StockHolding. Service Provider 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, Service Provider will be responsible for implementation of the Governance Model.

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

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

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

Service Provider has to develop a detailed transition plan covering at least the following key areas:

a) Transition Schedules, Tasks and Activities
b) Plan for Service Transition to new Service Provider
c) Transition activities like Service On-boarding, etc.
d) Operations and Support
e) Other Resources if any
f) Relationships to StockHolding's other Teams / Projects
g) Management Controls
h) Reporting Procedures
i) Risks and Contingencies- Key Risks, issues, dependencies and mitigation plans.

j) Transition Impact Statement and assessment
k) Review Process
l) Configuration Control
m) Plan Approval
n) Describe tools, methodologies and capabilities of the teams deployed for transition.

Service Provider is 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.
Transition Document	To be made available monthly for review.

Service Level Agreement (SLA) and Penalty

#	Activity	Description	SLA Threshold	Penalty	
1	Platform Availability and Notification Systems SLA	Service Provider will provide access to MDR platform and associated notification systems with the exception of "Scheduled Platform Maintenance". SLA for MDR Platform availability will be measured by the below formula: (Number of Minutes in the month system is available) x 100 / (Total number of minutes in the month)	99.90%	99.90 % and above	NA
				98% to 99.9	1 % of monthly contract value
				95% to 97.99%	2 % of monthly contract value
				90% to 94.99%	3 % of monthly contract value
2	Time to Notify customer on a High Severity Incident post first level investigation	The MDR Team will analyse alerts and create an Incident ticket for alerts that need action from the SOC Team. Such incidents will also be notified via email. The SLA for notifying High Severity Incident Tickets post first level investigation is 30 minutes after the alert is detected in MDR platform. SLA will be measured using formula: (Number of High Severity Incident Tickets notified within 30 minutes in a month) x 100 / (Total number of High Severity Tickets notified in a month) SLA is applicable only for High severity incident tickets.	95%	99.90 % and above	NA
				98% to 99.9	1 % of monthly contract value
				95% to 97.99%	2 % of monthly contract value
				90% to 94.99%	3 % of monthly contract value

		Definition: High Security Incident(s) is an indication of breach or has high likely hood of leading to breach/cause business disruption/high impact on assets, user. Examples: Ransomware, Large scale malware outbreak, Successful Phishing campaign, Confidential data exfiltration			
3	Time to provide remediation assistance to the customer on a High Severity Incident	For incidents that MDR SOC notifies, customer can contact SOC team for remediation assistance. The SLA to respond to such requests will be 60 minutes from time of request SLA will be measured using formula: (Number of Responses to High Severity Tickets Requests provided within 60 minutes in a month) x 100 / (Total number of High Severity Tickets Requests in a month) SLA is applicable only for responses to High severity incident tickets	95%	99.90 % and above	NA
				98% to 99.9	1 % of monthly contract value
				95% to 97.99%	2 % of monthly contract value
				90% to 94.99%	3 % of monthly contract value
4	Time to respond to the customer for Log data requests	On customer request, MDR SOC will retrieve and share log files related to an incident The SLA for retrieving log files for up to last 30 days is 6 hours from time of request	95%	99.90 % and above	NA
				98% to 99.9	1 % of monthly contract value
				95% to 97.99%	2 % of monthly

		SLA will be measured using formula: (Number of Log requests responded within 6 hours in a quarter) x 100 / (Number of Log requests) SLA is applicable only for log requests for up to last 30 days. For log requests greater than 30 days, there is no SLA. The response time will be communicated post assessment of the request.			contract value
				90% to 94.99%	3 % of monthly contract value
5	Publish Monthly MDR Operations Report	Monthly MDR SOC report will be delivered via email or stored in MDR platform every month, on or before the 10th business day. SLA will be measured using formula: Date of report delivery ≤10th business day This report will include a high-level summary information of SOC operations for the previous month	<=10th business day of the month	Rs. 5,000 for every days delay beyond the SLA Time period	
6	SIEM – MDR Implementation Go-Live	Go-Live of SIEM platform post integration with existing log collector and use cases (600 devices are on-boarded to the log collector)	Within 12 weeks from PO Acceptance	1% of One time Implementation Cost (Part A) for every weeks delay beyond the SLA time period	
7	Remaining Device On-boarding Go-Live	On-boarding of all remaining devices in scope	Within 24 weeks from PO Acceptance	1% of One time Implementation Cost (Part B) for every weeks delay beyond the SLA time period	

Contract Duration

1) Successful bidder shall enter into contract for the period of 03 (three) years.

Terms and Conditions

A. Payment:

SI.	Description	Payment Terms
1	One-time Implementation of SIEM Platform*	50% on SIEM – MDR Implementation Go-Live (Part A-600 devices to be on-boarded to the log collector) 50% on Remaining Device On-boarding Go-Live (Part B-600 devices to be on-boarded to the log collector)
2	SIEM Subscription + MDR Services	Monthly payment post adjustment of penalties if any for that quarter after SIEM – MDR Implementation Go-Live Milestone
*Note: One time Implementation performed for Part-A & Part-B needs to be duly authorized by StockHolding officials.		

Note:

a. Applicable penalty will / may be recovered from the monthly payment.
b. Applicable TDS and/or CESS will be recovered (deducted) from the payment.
c. First monthly Payment will be released only after signing of Integrity Pact and Non-Disclosure Agreement.
d. Payments will be released only after submission and verification of the required Bank Guarantee (BG). No payment will be made to successful bidder, until the BG verification is done.

B. Taxes & levies:

a. Applicable GST payable at actual as per prevailing rate of taxes as per Government notification
b. In case of tax exemption or lower TDS; Bidder has to submit letter from Government Authority for tax exemption or lower TDS (to be submitted along with each of the invoice(s) (c) Applicable TDS will be deducted from payment(s).

C. Bidder to abide by labour laws, human rights and regulations in their regions of business. Bidder to adhere to laws addressing child, forced or trafficked labour

Refund of Earnest Money Deposit (EMD):

a. EMD will be refunded through NEFT or return of BG/FDR to the successful bidder on providing an acceptance confirmation against the PO issued by StockHolding.
b. In case of unsuccessful bidders, the EMD will be refunded to them through NEFT or return of BG/FDR within 30 days after selection and confirmation of successful bidder, subject to internal approval of StockHolding.

Performance Bank Guarantee (PBG):

Successful Bidder shall, at own expense, deposit with the *StockHolding*, within Fifteen (15) days on issuance of PO, a Bank Guarantee (BG) for the value of 5% (Five per cent) of the Contract value (including GST) from scheduled commercial banks as per Annexure - 7. This Bank Guarantee shall be valid up to 60 days beyond the completion of the contract period. The BG claim period will be 12 months from BG expiry date. No payment will be due to the successful bidder based on performance, until the BG verification is pending. A penalty of ₹5,000 per day will be imposed on for any delay in issuing the PBG within the specified timeline

Bank Guarantee may be discharged / returned by *StockHolding* upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Bank Guarantee. *StockHolding* reserves the right to invoke the BG in the event of non-performance by the successful bidder.

Force Majeure

Neither StockHolding nor the Bidder shall be responsible for any failure to fulfil any term or condition of the CONTRACT if and to the extent that fulfilment has been delayed or temporarily prevented by a Force Majeure occurrence, defined as "Force Majeure". For purposes of this clause, “Force Majeure” mean an event beyond the control of the Parties and which prevents a Party from complying with any of its obligations under this Contract, including but not limited to: acts of God not confined to the premises of the Party claiming the Force Majeure, flood, drought, lightning or fire, earthquakes, strike, lock-outs beyond its control, labour disturbance not caused at the instance of the Party claiming Force Majeure, acts of government or other competent authority, war, terrorist activities, military operations, riots, epidemics, civil commotions etc.

The Party seeking to rely on Force Majeure shall promptly, within 5 days, notify the other Party of the occurrence of a Force Majeure event as a condition precedent to the availability of this defence with particulars detailed in writing to the other Party and shall demonstrate that it has taken and is taking all reasonable measures to mitigate the events of Force Majeure. And, all Parties will endeavor to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure. Each PARTY shall bear its own cost in relation to the force majeure occurrence.

However, any failure or lapse on the part of the Bidder to mitigate the damage that may be caused due to the above-mentioned events or the failure to provide adequate disaster management/recovery or any failure in setting up a contingency mechanism would not constitute force Majeure, as set out above.

If the duration of delay exceeds ninety (90) consecutive or one hundred eighty (180) cumulative days, StockHolding and the Bidder shall hold consultations with each other in an endeavour to

find a solution to the problem. Notwithstanding above, the decision of the StockHolding, shall be final and binding on the bidder.

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 Bidder complies with above-mentioned clause

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. We further understand and accept that StockHolding's decision in this regard will be final and binding on all bidders.

Integrity Pact

The Bidder will have to enter in to an Integrity Pact with StockHolding. The format (text) for the Integrity Pact is provided as Annexure-5. The Bidder will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory of the Bidder.

Non-Disclosure Agreement (NDA)

The successful Bidder will sign a Non-Disclosure Agreement (NDA) as per Annexure-8 with StockHolding for the contract period. The draft text of the NDA will have to be approved by legal department of StockHolding. All the expenses related to execution of the document such as the applicable stamp duty and registration charges if any shall be borne by the successful bidder.

Indemnify

The Bidder should hereby indemnify, protect and save StockHolding against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the Bidder. Any publicity by Bidder in which name of StockHolding is used should be done only with the explicit permission of StockHolding.

Subcontracting

As per scope of this RFP, sub-contracting is not permitted. The bidder shall not assign or sub-contract the assignment or any part thereof to any other person/firm.

Termination Clause

StockHolding reserves right to terminate the contract by giving **90 days** prior written notice in advance against any of the following conditions –

a) If penalty amount is equal to or more than 10% of monthly contract value for consecutively 3 times in a particular year;
b) If the SIEM solution implementation Go-Live exceeds 30 weeks' time period

c) If at any point of time, the services of bidders are found to be non-satisfactory;

Exit Management

a. Purpose: In the case of termination of the Contract, the Exit Management procedure should start 90 days before the expiry or termination of contract.
b. Plan: An Exit Management Plan, provided in writing by the Bidder to the StockHolding within 60 days of the acceptance of the Purchase Order/Contract, will outline the Bidder's support during the termination or expiration of the contract, along with the company's exit strategy. Following this, the exit plan must be reviewed and updated annually.
c. Bidder shall provide the Termination/Expiration Assistance regardless of the reason for termination or expiration.
d. Bidder shall fully and timely comply with the Exit Plan.
e. Bidder shall not make any changes to the Services under this Agreement and shall continue to provide all Services to comply with the Service Levels.
f. Confidential Information, Security and Data: The Bidder will promptly on the commencement of the exit management period supply to StockHolding the following:
    - Information relating to the current services rendered.
    - Documentation relating to Project's Intellectual Property Rights.
    - Project Data and Confidential Information.
    - All current and updated project data as is reasonably required for purposes of transitioning the services to its Replacement Bidder in a readily available format specified by StockHolding.

Assignment

Either Party may, upon written approval of the other, assign its rights and obligations hereunder to: (i) its Parent Corporation (as defined below) or an Affiliate; and (ii) a third party entity in connection with the transfer of all or substantially all of the business and assets of that party to such entity. For purposes of this Agreement, a "Parent Corporation" shall mean a company or entity owning over 50% of a Party and an "Affiliate" shall mean a company directly or indirectly controlling, controlled by, or under common control with, a Party. Except as provided above in this Section, either Party may assign its rights and obligations under this Agreement to a third party only upon receiving the prior written consent of the other Party, which consent may be reasonably conditioned but will not be unreasonably withheld or delayed. The Parties agree that no assignments will be made unless the assignee agrees to accept in full the responsibilities and obligations of the assigning Party.

ANNEXURE - 1 - Details of Bidder'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.

Sl. 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 of managing SIEM and MDR Services		
9	**Financial parameters**		
	Business Results (last three years)	Annual Turnover	Net Worth
		(Rs. in Crores)	(Rs. in Crores)
	2022-23		
	2023-24		
	2024-25		
	(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 2026

(Signature)

(In the capacity of)

ANNEXURE - 2 – Eligibility Criteria

To be submitted as part of
Technical Bid

SI. No	Criteria	Documents to be submitted by Bidder
1	The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of SIEM and MDR services implementation and support for the period of 7 years.	Copy of Certificate of Incorporation issued by the Registrar of Companies and Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory along with supporting documents for SOC related PO on or before RFP Date
2	The bidder should have an average annual turnover of at least Rs. 6 Crores per annum for last 03 (three) financial years (i.e. 2022-23, 2023-24 and 2024-25). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last three financial years.
3	The Bidder should have Positive Net worth minimum Rs. 2 crores for each of the last 03 (three) audited financial years (i.e. 2022-23, 2023-24 and 2024-25)	Certificate from CA mentioning networth for the past three financial years.
4	The bidder must have executed a minimum of three (03) projects related to SIEM and MDR services in India during the last five (05) years as of the RFP date, with at least one (01) deployment handling not less than 2000 EPS (Events Per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution. Note: Bidder to submit the experience of proposed SIEM and MDR tool only for this RFP.	Copy of Purchase Order /Completion certificate with Customer Name and Address, Contact Person, Telephone Nos. Fax and e-mail Address and customer reference to be provided
5	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 3 years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
6	The bidder must possess at the time of bidding, following valid certifications: ISO 9001:2008 or latest/ISO 20000 or ISO 27001:2013 or latest	Relevant valid ISO Certificates
7	The bidder must have a direct partnership with the supplier of the SIEM tool. One Service	MAF from OEM to be submitted

	Provider can bid only with one OEM as regards SIEM solution is concerned	
8	Bidder should have Support office at MMRDA Region or Pune.	Bidder to provide office address along with GST details.
9	The Bidder to submit signed & stamped Integrity Pact as per Annexure - 5	Self-declaration by authorized signatory of Bidder

Note:

a. Letter of Authorization shall be issued by either Managing Director having related Power of Attorney issued in his favour or a Director of the Board for submission of Response to RFP
b. All self-certificates shall be duly signed and Stamped by Authorized signatory of the Bidder Firm unless specified otherwise.
c. Bidder response should be complete, Yes/No answer is not acceptable.
d. Details of clients and relevant contact details are mandatory. Bidders 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 2026
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE – 3 – Technical Criteria & Compliance

The proposal submitted by the bidders shall, therefore, be evaluated on the following criteria:

Sl. No	Parameter	Scores	Max Scores
A. **BASED ON VENDOR TURNOVER & EXPERIENCE (70 MARKS)**			
1	Average annual turnover of the bidder during last 03 (three) years (i.e. 2022-23, 2023-24 and 2024-25)	• 6 Crores >= 10 Crores : 10 Marks • >10 Crore but <= INR 15 Crore : 12 Marks • More than INR 15 crore : 15 Marks	15
2	Projects for implementation of SIEM and MDR services with at least 1 deployment not less than 2000 EPS (Events per Second) or a minimum integration of 1000 devices with the deployed SIEM-MDR solution each during last 05 (five) years in India Note: Bidder to submit the relevant experience only of the SIEM and MDR tool proposed for this RFP.	• 1-3 Projects – 10 Marks • 4-5 Projects – 12 Marks • More than 5 Projects – 15 Marks	15
3	Projects of SIEM and MDR services implementation in BFSI Sector in India during last 05 (five) years in India	• 1-3 Projects – 5 Marks • 4-5 Projects – 7 Marks • More than 5 Projects – 10 Marks	10
4	OEM solution must be positioned in the respective Leader's quadrant/category of the latest IDC MarketScape or Gartner Magic Quadrant, or Forrester Wave reports for proposed SIEM Solution	Presence of OEM Solution in Leader's quadrant/category – 10 Marks	10
5	The bidder should have minimum three (3) resources certified/ trained on the proposed SIEM solution.	The bidder must submit relevant certifications or details of the trained resources. Evaluation will be based on the number of certified/trained resources provided, as follows: 3 resources – 4 Marks 4 to 5 resources – 6 Marks More than 5 resources – 8 Marks	8

6	Customer reference for proposed SIEM-MDR Solution during the last 5 years as on RFP date	3 Customer reference Feedback from existing customer 2 = Average, 3 = Good, 4 = Excellent	12
B. **TECHNICAL PRESENTATION (30 MARKS)**			
7	Bidder's technical presentation	• Understanding of the Project requirements – 5 marks • OEM/Bidder's SIEM and MDR Implementation Capabilities – 5 marks • Relevant Experience in managing SIEM and MDR Solution – 5 marks • Proposed SIEM and MDR Features - 10 marks • Approach and Methodology of solution implementation and SLA management – 5 marks	30

Note:

- The bidder is required to provide documentary evidence for each of the above criteria.
- StockHolding shall verify the credentials submitted with the respective issuer and understand the credentials claimed for the purpose of evaluation and awarding marks.
- The bidder to submit appropriate credentials [other than self- certification] in respect of each of the item.
- Technical proposals will be evaluated based on the total marks obtained across all technical evaluation criteria. Only those bidders who achieve a minimum cumulative score of 60 marks in the technical evaluation will qualify for the commercial bid evaluation.

Technical Compliance:

The bidder is required to submit a response along with solution document by responding to the above requirements with "Yes" or "No". The same should be submitted along with the bid documents. StockHolding reserves the right to reject the bid based on any Non-compliance to below Technical requirements.

Security Information and Event Management

Sr. No.	Capabilities	Compliant (Y/N)	Evaluation Marks (0 Marks if Compliance = N)

	Expectation from Managed Detection and Response (MDR) Services		
1	High Speed Threat Detection and Response: AI platform and threat hunters continuously scan our entire IT stack for threats and deliver high speed defence for us. Early detection capabilities clubbed with speedier response helps pre-empt and combat known and unknown threats proactively. No Half-Measures in Defending the Cyber Assets: MDR offering to provide for all six components of threat management – intelligence, analytics, SIEM, forensics, cyber incident remediation, and breach management—to protect StockHolding's critical infrastructure and networks. Low Noise, High Touch Service: Traditional SIEM-based security monitoring cannot detect complex, targeted, or unknown attacks. It is unable to analyse a high volume of varied data. In short: it is unable to defend StockHolding from next-generation cyber-attacks. Security professional along with AI platform, can provide validated threats and high touch response services, to StockHolding.		
	Solution Implementation		
2	SIEM solution shall be implemented in Service Provider's Data Centre or Cloud based. The Service Provider shall ensure that Data Centre / Cloud Service shall be hosted in India and in no circumstances data shall not move out of India during the entire contract duration.		
3	Service Provider's MDR Team shall be based offshore – out of Service Provider's offices.		
4	Implement the SIEM tool to collect logs from the identified devices / applications / databases etc.		
5	Provide and/or develop parsing rules for standard/ non-standard logs respectively.		
6	Implement correlation rules based on out-of-box functionality of the SIEM solution and also based on the use-cases identified.		
7	Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool.		
8	Build custom interfaces/ Connector for Applications. To begin with StockHolding will start with integration of critical applications. Service Provider can be asked for integrating further more applications if found critical and required by StockHolding.		
9	While, it is expected that connectors for all the standard applications and devices will be readily available with the Service Provider and connector for mostly in-house/custom built applications will need to be developed. Service Provider is be expected to develop connector for the custom built applications specifically developed for StockHolding.		

10	The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by StockHolding as per the SOW including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations i.e. DC, DR and branch offices, etc.		
11	The solution should be able to handle at least 2000 sustainable EPS and scalable to 5000 Peak EPS.		
12	The MDR team shall coordinate with StockHolding's SOC Team to on-board and integrate as per the requirement of devices on boarded with MDR.		
13	Selected Bidder will customize incident management / dashboard / reports for StockHolding and will modify the same as per the changing requirement of StockHolding.		
14	Bidder will also supply all the necessary hardware, software and supporting accessories etc. for integration of the components supplied for CSOC. REC will supply only the Rack space, power and network points.		
15	The proposed solution shall have storage for managing and storing logs from various devices. Storage should provide minimum 180 days		
	Log Collection		
16	Logs from all the in-scope devices and additional devices integrated as part of contract period located at the geographically dispersed location should be collected. Bidder / Vendor should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. The log baseline should be in line with industry best practices. In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer. Only in case where remote log collection is not feasible, bidder / vendor should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement. Prepare Daily, Weekly, Monthly compliance reports.		
	Log Correlation		
17	Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by the bidder on regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents.		
	Alert Generation		
18	Solution should be capable to generate alerts, register and send/receive the same through message formats like SMTP, SMS, Syslog, and SNMP as per user configurable parameters		
	Event viewer / dashboard / reports / incident management		
19	SIEM Solution should provide web-based facility to view security events and security posture of the StockHolding's Network and		

	register incidents. Solution should have drill down capability to view deep inside the attack and analyze the attack pattern. Dash board should have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc. Dashboard should have Role based as well as Discretionary access control facility to restrict access to incidents based on user security clearance level. Solution should provide various reports based on user configurable parameters and standard compliance reports like ISO27001, IT Act and regulatory reports. Selected bidder will customize incident management / dashboard / reports for StockHolding and will modify the same as per the changing requirement of StockHolding.		
	Incident Management Tool		
20	The principal goal of the incident management process is to identify anomalous activities in the environment, contain those events and restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus facilitating continued service quality and availability.		
21	Solution should be able to register any security event and generate trouble ticket.		
22	Solution should provide complete life cycle management (work flow) of trouble tickets from incident generation till closure of the incident.		
23	Bidder should also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate/remediate, recover and learn from the incidents responded to.		
24	Solution should provide the logging facility to different levels of users to monitor and manage the incidents generated for closure of the same as per the defined workflow.		
25	Solution should be able to integrate with different tools such as SIEM tool, Vulnerability Management tool etc. Incident management should include escalation as per the escalation matrix. However, it is preferred that the SIEM should have an inbuilt integrated incident management tool.		
26	Develop workflow for incident management tool and be responsible for end to end incident management lifecycle.		
	Managed Detection and Response Services		
27	24x7 monitoring of security alerts (from SIEM), prioritizing and notifying high priority alerts.		
28	Provide Assistance for StockHolding's compliance needs- like ISO 27001:2022 or latest, SOC2 Type 2 Audits etc. and internal policy violations in standard formats.		
29	Investigation on potential incidents and high priority alerts.		
30	Raising remediation tickets to pre-defined users with recommendations and/or response playbooks		
31	24x7 access to security operations personnel over email, voice and video calls and chats.		

32	Publishing Monthly MIS report based on predefined dashboards and reports.		
	Brief description of how operations are performed post Implementation		
33	Security Monitoring: Service Provider starts the MDR Remote Log Monitoring service upon successful implementation of technology/platform. The alerts generated on Alerting Sources (SIEM, RCE, IPS, EAF, etc.) are fed in to MDR platform and investigated for who, what, when, and how to determine extent of the impact.		
34	Service Provider's MDR offering validates the threats and provides deep incident analysis combining their platform with specialized incident responders. As part of the service, triaging of alerts begin to focus on the most relevant threats and then investigates them to establish if there is a security incident. All the relevant evidences and artefacts related to investigation are stored and maintained in the platform. Alerts are converted into more significant information such as the attack chain, blast radius, and potential impact to assets.		
35	Threat Anticipation: This is threat intelligence in action, and tailored threat anticipation goes far beyond traditional passive threat intelligence feeds available. Global threat intelligence is applied in StockHolding's specific context to enhance our protection. A key part of the MDR service from Service Provider is to gather data and intelligence on threats and attacks worldwide, and to then distil the information to identify which customers might be affected. Service Provider's Threat Anticipation Service is designed to help us stay protected from the latest threat and vulnerabilities by providing actionable inputs related to Vulnerability, Threat and Threat Intel. The TA feed is sent from Service Provider's Intel. Threat Intelligence component of TA feed is fed directly into the MDR platform and is tracked and closed for implementation delivering Actionable Threat Anticipation i.e. From Security News to Protection within Hours.		
36	Auto Containment: Service Provider's auto remediation to quickly contain threats by enabling rules on firewall, NGFW, IPS, Proxy, EDR, WAF, Patch management, Routers or AD. Service Provider will integrate our security devices and push rules based on pre-defined response playbooks, for us. Incase auto-remediation is not possible, Service Provider to coordinate with StockHolding's SOC Team to manually apply the changes.		
37	Threat Hunting: Threat hunting advocates – "Don't wait for alerts to show up; hunt them". Output of advanced security analytics models run on the platform which is analyzed by a specialized hunting team and the data is queried further to detect threats that may have bypassed other security controls or use cases. This is security analytics in action: MSSP should apply data science and machine learning models to network, application, user, and machine data to proactively hunt for unknown and hidden threats in our environment.		
38	As a part of the Standard MDR offering, Service Provider should detect, investigate and contain threats. Post that, they will send out		

	tickets to StockHolding's SOC team for mitigation and response actions within our network. They will also provide playbooks and knowledge base to help us resolve these tickets. StockHolding's SOC team can reach back to them for query resolution but such support is provided on best effort basis.		

Security solutions to be integrated with SIEM Platform

Sr. No.	Capabilities	Compliant (Y/N)	Evaluation Marks (0 Marks if Compliance = N)
39	Security solutions to be integrated with SIEM, but not limited to the below list. The below inventory could change depending upon installation of new systems and components based on StockHolding's requirements, during the course of the period of assignment. The Service Provider chosen shall, however, undertake to support / such new additions to the infrastructure also at no additional cost to StockHolding. ▪ WAF Web Application Firewall ▪ NAC Network Access Control ▪ Perimeter Firewall and Intrusion Prevention System (IPS) ▪ Brand Protection and Monitoring Logs, Website Monitoring Service against Defacement ▪ Anti-Phishing Service Logs ▪ Packet Analysis ▪ Database and Compute Server Audit Logs ▪ End Point Protection ▪ Active Directory Logs ▪ Oracle NSG and VMWare NSX Logs ▪ Application Delivery Controller (ADC) Logs ▪ PIM, PAM, CISCO ISE Logs, CISCO ESA logs, ▪ Routers and Switches ▪ Proxy ▪ Oracle Exadata and PCA ▪ VMware Private Cloud		

Deliverables

Sr. No.	Capabilities	Compliant (Y/N)	Evaluation Marks (0 Marks if Compliance = N)
	Managed Detection and Response Sizing and Capabilities		
40	Project Initiation and Transition: As a part of the project initiation phase, Service Provider's program manager will conduct a Kickoff meeting and provide walkthrough of scope, pre-requisites, implementation plan, task management tool, escalation Matrix and Governance Model.		

	Service Provider will provide and follow an agile approach for Integration of log sources. Their methodology is described below: ▪ Critical First - Critical log sources are monitored first. This will reduce the risk of breach. ▪ Incremental Value – Phase wise approach will ensure StockHolding see incremental value. ▪ Continuous Improvements – Learnings from every phase can be deployed in the latter phases. ▪ Quick value realization – StockHolding will be able to see the value of the service at high speed and not wait for all log sources. Service Provider will deliver: ▪ Unified Tool - One click access to program Status. Access and demo will be provided during the pre-kick off discussion. ▪ Accountability - All tasks of the project are assigned on Service Provider's tool with a due date. The Managed Service team and MDR tasks are assigned on the tool. ▪ Dashboard - Risks, dependencies, milestones, and work progress can be viewed in a single click – anytime and anywhere transparency		
	Support for Managed Detection and Response Services (MDR Services)		
41	**Log Collection:** Logs from all the in-scope and other StockHolding Servers and network devices located at the geographically dispersed location should be collected. Service Provider 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, Service Provider 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, Service Provider 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. Existing Raw logs should also be accessible in SIEM platform, additionally collectors to be made available as per stockholding list of Devices and use cases.		
42	**Logging of Critical Devices**		

	a) The Service Provider is required to maintain the syslog of the devices installed at DC, DR and NDR locations for a period of 180 days. b) The logs will be reviewed by StockHolding officials on quarterly and half yearly basis and same has to be ensured by Service Provider. c) Service Provider will design and implement all simple scripts that may be needed to analyse logs and produce reports as required by StockHolding officials.		
43	**Logging of Critical Devices:** 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. Collected logs should be encrypted and compressed before the transmission to the remote Log Correlation Engine.		
44	**Log Archival:** Logs collected from all the devices should be stored in a non-tamper able format on the archival device in a 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 180 days log data should be available online. Logs prior to 180 days period should be stored on removable media. Service Provider will ensure that retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols.		
45	**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. Service Provider will coordinate with StockHolding SOC 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.		
46	**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. Service Provider has to ensure that all such alert mechanisms are intact and brought to the notice of StockHolding team during their tenure on immediate basis to ensure compliance.		
47	**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. Service Provider's 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 shall 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 latest regulatory reports. Service Provider has to ensure that StockHolding should get all the configured reports to ensure compliance. Service Provider 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 Service Provider.		
48	**Integration with in-scope monitored devices** Service Provider's 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.		
49	**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.		
50	**Workflow Automation** Service Provider will define the work flow automation so that applications are integrated and manual intervention is minimal.		
51	**Integration of devices in Managed detection and response along with SIEM Services:** a) Integrate the devices with MDR and SIEM to collect logs from the identified devices, applications, and databases etc. b) Develop parsing rules for non-standard logs. c) Implement correlation rules of the SIEM solution/ service design provided by MDR team. d) 24X7X365 log monitoring for in scope devices and applications. e) Rapid real-time response to incidents. f) Evaluation of incidents. g) Forensics to identify the origin of threats, mitigation thereof, initiation of measures to prevent recurrence. h) The SIEM solution/ service shall also have capability such that StockHolding Team can also execute the queries to identify custom made scenarios/incidents.		

Dated this..... Day of 2026
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE - 4 - Commercial Price Bid Format

Commercial Price Bid Format

SI.	Description	Year 1 Cost	Year 2 Cost	Year 3 Cost
1	One time Implementation of SIEM Platform	Required	-	-
2	SIEM Subscription + MDR Services	Required	Required	Required
Total Cost without GST				
GST Charges (₹)				
Total 3 Years Cost with GST (₹)				

Note:

a. Price to be quoted is for 03 (three) years including GST while uploading financial bids on GeM portal.
b. Applicable penalty will / may be recovered from the monthly payment.
c. Bidder must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. 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.
d. No additional cost shall be paid for custom development of any adapters for integration with SIEM Solution.
e. List of Applications mentioned in the RFP are as of present today and might increase in the future. Any additional applications to be on-boarded shall be at zero cost to StockHolding.

ANNEXURE - 5 – Integrity Pact

(_____ Name of the Department / Office) RFP No._____ 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. B 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. Bidders 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 Bidder(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 Bidder(s)/Counter Party(ies) with equity and reason. The Principal / Owner will, in particular, before and during the Tender (RFP) Process, provide to all Bidder(s) / Counter Party (ies) the same information and will not provide to any Bidder(s)/Counter Party (ies) confidential / additional information through which the Bidder(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/Bidders

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) / Bidders 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, favour, 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, favour, 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 favour or disfavor to any person in relation to the contract or any other contract with the Principal / StockHolding.

4. Bidder / Counter Party shall disclose the name and address of agents and representatives, if any, handling the procurement / service contract.
5. Bidder / 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 Bidder / Counter Party has to further confirm and declare to the Principal / StockHolding that the Bidder / 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 Bidder / 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 Bidder / Counter Party has to submit a Declaration along with Eligibility Criteria, as given at **Annexure**. If bids are invited through a Consultant a Declaration has to be submitted along with the Eligibility Criteria as given at **Annexure**.
8. The Bidder / 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 Bidder / 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 Bidder / Counter Party shall not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
11. The Bidder 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, proposals and business details, including information contained in any electronic data carrier. The Bidder / Counter Party also Undertakes to exercise due and adequate care lest any such information is divulged.
12. The Bidder / 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 Bidder / 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 Bidder / Counter Party or any employee of the Bidder or any person acting on behalf of the Bidder / 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 Bidder's / Counter Party firm, the same shall be disclosed by the Bidder / 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 Bidder / 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 Bidder / 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 Bidder / Counter Party exclusion from the Tender (RFP) Process.
18. The Bidder / Counter Party agrees that if it makes incorrect statement on this subject, Bidder / 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 Bidder(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 Bidder / Counter Party / Contractor from the Tender (RFP) Process or terminate the Contract, if already executed or exclude the Bidder / 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 Bidder / 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 Bidder / Counter Party / Contractor as deemed fit by the Principal / Owner / StockHolding.
4. The Bidder / 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 Bidder / Contractor(s) / Counter Party:-

1. Forfeiture of EMD / Security Deposit : If the Principal / StockHolding / Owner has disqualified the Bidder(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 Bidder / Contractor / Counter Party.

2. Criminal Liability: If the Principal / Owner / StockHolding obtains knowledge of conduct of a Bidder / Counter Party / Contractor, or of an employee of a representative or an associate of a Bidder / 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.

IV. Equal Treatment of all Bidders/Contractors / Subcontractors / Counter Parties

1. The Bidder(s) / Contractor(s) / Counter Party (ies) undertake (s) to demand from all subcontractors a commitment in conformity with this Integrity Pact. The Bidder / Contractor / Counter-Party shall be responsible for any violation(s) of the principles laid down in this Agreement / Pact by any of its sub-contractors / sub-bidders.
2. The Principal / StockHolding / Owner will enter into Pacts on identical terms as this one with all Bidders / Counterparties and Contractors.
3. The Principal / StockHolding / Owner will disqualify Bidders / Counter Parties / Contractors who do not submit, the duly signed Pact, between the Principal / Owner / StockHolding and the Bidder/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 Shri Shekhar Prasad Singh, IAS (Retd.) as 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, StockHolding Ltd.
3. The Bidder(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) / Bidder / Counter Party. The Counter Party / Bidder / 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-Contractors Tender (RFP) Documentation / papers / files. The IEM is under contractual obligation to treat the information and documents of the Bidder(s) / Contractor(s) / Sub-Contractors / Counter Party (ies) with confidentiality.
4. In case of tender (RFP)s having value of 50 lakhs 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 nonbinding 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 / Bidder, 12 months after the completion of work under the Contract, or till continuation of defect liability period, whichever is more and for all other Bidders, 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 the 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 WITHNESS 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 Bidder / 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 – 6 – Compliance Statement

(To be submitted on Company Letter Head)

Subject: **RFP REF NO:** CPCM-03/2026-27 dated 09-Apr-2026 for Selection of Service Provider for Implementation and Support of SIEM and MDR Services for Stockholding

DECLARATION

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

Sr. No.	Item / Clause of the RFP	Compliance (Yes / No)	Remarks/Deviations (if any)
1	Objective of the RFP		
2	Scope of Work		
3	Eligibility Criteria		
4	Service Level Agreement (SLA) / Scope of Work		
5	Non-Disclosure Agreement		
6	Payment Terms		
7	Bid Validity		
8	Integrity Pact		
9	All General & Other Terms & Conditions in the RFP		
10	Technical Compliance		

(If Remarks/Deviations column is left blank it will be construed that there is no deviation from the specifications given above)

Date: Signature with seal

Name & Designation:

ANNEXURE – 7 – Format of Bank Guarantee

This Bank Guarantee is executed by the ---------- (Bank name) a Banking Company incorporated under the Companies Act, 1956 and a Scheduled Bank within the meaning of the Reserve Bank of India Act, 1934 and having its head office at ---------- and branch office at _____(hereinafter referred to as the "Bank", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) and Branch office at _____ in favour of Stock Holding Corporation of India Limited, a Company incorporated under the Companies Act, 1956 and having its Registered Office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400 012 (hereinafter referred to as "StockHolding", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) at the request of _____, a Company incorporated under the Companies Act, 1956 and having its Registered Office at (hereinafter referred to as the "Service Provider", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns).

Whereas

A. StockHolding has, pursuant to the Tender No. _____, issued the Purchase Order dated _____ to the Service Provider for providing _____
B. In terms of the said Tender, the Service Provider has agreed to furnish to StockHolding, a Bank guarantee for Rs. _____ /- (Rupees _____ only) till _____ (date).
C. The Bank has, at the request of the Service Provider**,** agreed to give this guarantee as under.

NOW IN CONSIDERATION OF THE FOREGOING:

1. We, the Bank, at the request the Service Provider, do hereby unconditionally provide this guarantee to StockHolding as security for due performance and fulfilment by the Service Provider of its engagements, commitments, operations, obligations or liabilities including but not limited to any sums / obligations / claims due by the Service Provider to StockHolding for meeting, satisfying, discharging or fulfilling all or any obligation or liability of the Service Provider, under the said Tender / Purchase Order.

2. We, the Bank, hereby guarantee and undertake to pay StockHolding up to a total amount of Rs. _____/- (Rupees _____ only) under this guarantee, upon first written demand of StockHolding and without any demur, protest and without any reference to the Service Provider**.**
3. Any such demand made by StockHolding shall be conclusive and binding on the Bank as regards the amount due and payable notwithstanding any disputes pending before any court, Tribunal, or any other authority and/ or any other matter or thing whatsoever as the liability of the Bank under these presents being absolute and unequivocal.
4. We, the Bank, agree that StockHolding shall have the fullest liberty without consent of the Bank to vary the terms of the said Tender/ Purchase Order or to postpone for any

time or time to time exercise of any powers vested in StockHolding against the Service Provider and to forbear or enforce any of the Terms & Conditions relating to the said Tender / Purchase Order and the Bank shall not be relieved from its liability by the reason of any such variation, or extension being granted to the Service Provider or for any forbearance, act or omission or any such matter or thing whatsoever.

5. We, the Bank, agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged.
6. This Guarantee shall not be affected by any change in the Constitution of the Bank or the Service Provider or StockHolding.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN ABOVE:

1. The liability of the bank under this guarantee is restricted to a sum of Rs. _____/- (Rupees _____ only).
2. This Bank Guarantee will be valid for a period up to _____ (date).
3. A written claim or demand for payment under this Bank Guarantee on or before _____ (date) is the only condition precedent for payment of part/full sum under this guarantee.

For Issuing Bank

Name of Issuing Authority:

Designation of Issuing Authority:

Employee Code:

Contact Number:

Email ID:

ANNEXURE – 8 – Format of Non-Disclosure Agreement

This Non-Disclosure Agreement (hereinafter "Agreement") is executed on this _____ day of _____, **20xx** by and between

Stock Holding Corporation of India Limited, a company incorporated under the Companies Act, 1956 and having its registered office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400012 (hereinafter referred to as "**StockHolding**" which expression shall mean and include its successors and assigns), of the One Part;

And

Company Name, a company incorporated under the Companies Act, 1956 and having its registered office / corporate office at **Complete Address** (hereinafter referred to as "**Company Name**" which expression shall mean and include its successors and assigns), of the Other Part.

(StockHolding and **Company Name** are individually referred to as 'Party' and collectively as 'Parties'.)

The Party disclosing Confidential Information under this Agreement shall be referred to as Disclosing Party and the Party receiving Confidential Information shall be referred to as Receiving Party.

1. **Purpose**: Whereas, the Parties wish to explore possible business opportunity, during which either Party will be required to disclose certain Confidential Information to the other.
2. **Confidential Information and Exclusions**: Confidential Information shall mean and include (a) any information received by the Receiving Party which is identified by Disclosing Party as confidential or otherwise; (b) all information including technical, data security , cyber security business, financial and marketing information, data, 80
3. analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, know-how, ideas, concepts, strategies, trade secrets, product or services, results obtained by using confidential information, prototype, client or vendor list, projects, employees, employees skills and salaries, future business plans disclosed by Disclosing Party whether orally or as embodied in tangible materials. Confidential Information shall however exclude any information which a) is in the public domain; (b) was known to the Party of such disclosure or becomes known to the Party without breach of any confidentiality agreement; (c) is independently developed by the Party without use of Confidential Information disclosed herein; (d) is disclosed pursuant judicial order or requirement of the governmental agency or by operation of law, provided that the recipient party gives disclosing party a written notice of any such requirement within ten (10) days after the learning of any such requirement, and takes all reasonable measure to avoid disclosure under such requirement.
4. **Confidentiality Obligations**: The Receiving Party shall, at all times maintain confidentiality and prevent disclosure of Confidential Information of Disclosing party with at least the same degree of care as it uses to protect its own confidential information but in no event with less than reasonable care. The Receiving Party shall keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party. The Receiving Party agrees not to disclose, transmit, reproduce or make available any such Confidential

Information to any third parties and shall restrict disclosure of Confidential Information only to a limited group of Recipient's directors, concerned officers, employees, attorneys or professional advisors who need to have access to the Confidential Information for the purposes of maintaining and supporting the services and each of whom shall be informed by Receiving Party of the confidential nature of Confidential Information and agree to observe the same terms and conditions set forth herein as if specifically named a Party hereto. The Receiving Party shall not, unless otherwise agreed herein, use any such Confidential Information and Confidential Materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects. The Receiving Party shall not use the Confidential Information in any way to create a derivative work out of it or reverse engineer or use for any commercial purpose or for any purpose detrimental to the Disclosing Party. The Receiving Party shall not make copies of Confidential Information unless the same are reasonably necessary. The Receiving Party shall immediately notify Disclosing Party in the event of any unauthorized use or disclosure of the Confidential Information and reasonably support Disclosing Party in taking necessary remedial action.

5. **No Warranty**: All Confidential Information is provided 'as is.' Neither Party makes any warranty, express, implied or otherwise, regarding its accuracy, completeness or performance.
6. **No License**: Each Party recognizes that nothing in this Agreement is construed as granting it any proprietary rights, by license or otherwise, to any Confidential Information or to any intellectual property rights based on such Confidential Information.
7. **Return**: The Receiving Party who receives the Confidential Information and Confidential Materials agrees that on receipt of a written demand from the Disclosing Party:
    a. Immediately return all written Confidential Information, Confidential Materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control; (SUCH RETURN OF DOCUMENTS SHOULD BE DONE BY SIGNING A LETTER).
    b. To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;
    c. So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and
    d. To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.
    e. Receiving party will attempt to maintain, to the best possible extent, physical and logical segregation of the Confidential Information of the data of the Receiving party from data of any third party.
8. **Term**: The term of this Agreement shall be ____ (___) years from _____ (the Effective Date). Either Party may terminate this Agreement by giving a thirty (30) days

written notice to the other. The confidentiality obligations stated in this Agreement shall survive for a period of three (3) years from the date of termination or expiration of this Agreement.

9. **Remedies**: The Confidential Information and Confidential Materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.
   The Parties acknowledge and agree that the Disclosing Party will suffer substantial and irreparable damage, not readily ascertainable or compensable in monetary terms, in the event of any breach of any provision of this Agreement by the Receiving Party. The Receiving Party therefore agrees that, in the event of any such breach, the Disclosing Party shall be entitled, without limitation of any other remedies otherwise available to it, to obtain an injunction or other form of equitable relief from any court of competent jurisdiction.
10. **Governing Law and Jurisdiction**: This Agreement may be governed and construed in accordance with the laws of India and shall be subject to the jurisdiction of courts in Mumbai, India.
11. **Miscellaneous**: This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior commitments/ understanding in this regard and may not be amended or modified except by a writing signed by a duly authorized representative of the respective Parties. This Agreement may be executed in several counterparts (physical or electronic form), each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. This Agreement may not be assigned or transferred except by a mutual written consent of both the Parties.

For Stock Holding Corporation of India Limited	**For Company Name**
Name:	Name:
Title:	Title:
In the Presence of	
Name:	Name:
Title:	Title: