Stock Holding Corporation of India Limited

(StockHolding)

RFP Reference Number: CPCM-07/2025-26

Date: 02-Jul-2025

GEM Reference No. - GEM/2025/B/6402236

Request for Proposal (RFP) for Procurement of Cloud based Web Application and API Protection (WAAP)

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-07/2025-26
3	Requirement	RFP for Procurement of Cloud based Web Application and API Protection (WAAP)
4	Interest free Earnest Money Deposit (EMD) [*]	Rs.10,50,000/- (Indian Rupees Ten Lakhs Fifty Thousand only) by way of RTGS/NEFT to be paid to Stock Holding Corporation of India Limited as Earnest Money Deposit should be submitted separately before submission of online bids by way of RTGS/NEFT on 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 and Medium Enterprises (MSME) 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	02-Jul-2025
7	Date, Time and place for online Pre-bid meeting	04-Jul-2025 11:00 AM For participation in pre-bid meeting, please send mail for online meeting link to CPCM@stockholding.com before 03-Jul-2025 05:00 PM
8	Last Date for Submission of Online Bid	14-Jul-2025 03:00 PM
9	Date of opening bid	14-Jul-2025 03:30 PM

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 6
ELIGIBILITY CRITERIA (Documents to be Submitted Online) 8
BIDS PREPARATION AND SUBMISSION DETAILS 10
Submission of Bids 10
Evaluation of Bids 10
REQUIREMENT 14
Scope of Work 14
Service Level Agreement (SLA) and Penalty 19
Delivery Timelines 21
Terms and Conditions 21
Contract Duration 22
Refund of Earnest Money Deposit (EMD) 22
Performance Bank Guarantee (PBG) 22
Force Majeure 23
Dispute Resolution 24
Right to alter RFP 24
Integrity Pact 24
Sub-Contracting 24
Non-Disclosure Agreement (NDA) 24
Indemnify 24
Termination Clause 24
Exit Management 25
Assignment 25
ANNEXURE - 1 - Details of Bidder's Profile 26
ANNEXURE - 2 – Eligibility Criteria 27
ANNEXURE - 3 – Technical Criteria 29
ANNEXURE - 4 - Commercial Price Bid Format 31
ANNEXURE - 5 – Integrity Pact 33
ANNEXURE - 6 - Covering Letter on bidder's Letterhead of Integrity Pact 40
ANNEXURE – 7 – Compliance Statement 41
ANNEXURE – 8 – Format of Bank Guarantee 42
ANNEXURE – 9 – Format of Non-Disclosure Agreement 44
ANNEXURE – 10 – Technical Compliance 47

SUBMISSION OF PROPOSAL

StockHolding invites e-tender through GeM Portal, in two bid system (Technical and Commercial bid), for Procurement of Cloud based Web Application and API Protection (WAAP) for 03 (three) years at StockHolding.

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. Eligibility/Technical Bid (.pdf files)
2. Commercial Bid (.pdf files)

Invitation for bids:
This "Invitation for bid" is meant for the exclusive purpose of "Procurement of Cloud based Web Application and API Protection (WAAP) for 03 (three) years at 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.

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 Format for Eligibility Criteria - Annexure 2
c Format for Eligibility Criteria – Annexure 3
d Format for Commercial Bids - Annexure 4
e Integrity Pact (Text) - Annexure 5
f Covering Letter of Integrity Pact - Annexure 6
g Compliance Statement – Annexure 7
h Format of Bank Guarantee – Annexure 8

i Format of Non-Disclosure Agreement (NDA) – Annexure 9
j Technical Compliance - Annexure 10

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 obtain such clarifications 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 right 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's/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.

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)

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 registered Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 with experience in providing similar services for past 3 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
2	Bidder should have an average annual turnover of at least ₹ 2.8 Crores per annum for last three financial years (2021-22, 2022-23 and 2023-24). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last three financial years.
3	Bidder should have Positive Net worth (minimum ₹1.05 crores) for all the last 03 (three) audited financial years	Certificate from CA mentioning net worth for the past three financial years.
4	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 2 years from the RFP date.	Self-declaration by the bidder on its Letter Head duly signed by the Authorized Signatory
5	The bidder should be the OEM or partner of the OEM for the proposed WAAP	The bidder should provide Manufacturer's Authorization Letter (MAF). If bidder is OEM itself, MAF not required.
6	The bidder should have at least 03 (three) successful implementations in India of the proposed WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date	Copy of order and/ or completion certificate of work
7	The proposed OEM should have ISO 27000 and/or SOC2 Type2 series certifications	Copy of valid certifications
8	OEM should have WAF services hosted from India Data center only and the WAF Inspection should not happen outside India for traffic generated in India during the entire contract period.	Self-declaration by the bidder on its Letter Head duly signed by the Authorized Signatory

9	OEM's Data Centre shall not be in public cloud i.e. Azure, GCP and AWS	Self-declaration by the bidder on its Letter Head duly signed by the Authorized Signatory
10	Bidder shall have support office in MMR region	Bidder to provide office address along with GST details

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.

Submission of Bids

1) 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
2) The offer should be valid for a period of at least **90 days** from the date of submission of bid.
3) 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.
4) 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.
5) Delayed and/or incomplete bid shall not be considered.
6) 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.

Evaluation of Bids

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 (Stage 1)

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.

Technical Bid Evaluation (Stage 2)

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. 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	Min. Scores	Max. Scores
	A. Experience of Bidder & Proposed Solution (70 Marks)			
1	The bidder should have at least 03 (three) successful implementations in India of the WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date	• 3 projects : 10 Marks • 4-5 Projects: 15 marks • More than 5 Projects: 20 Marks	10	20
2	OEM solution must be positioned in the Leaders Quadrant of the latest IDC MarketScape, Gartner Magic Quadrant, or Forrester Wave reports for Web Application Firewall and API Protection.	Presence of OEM Solution in Leader's Quadrant – 10 Marks	0	10
3	Technical Compliance for Solutions	Based on the features mentioned in Annexure-10	30	40
	B. Presentation & Solution Demonstration (30 Marks)			
4	OEM proposed solution Use Cases that needs to be demonstrated during the Demo session are mentioned below: 1. Protection Against OWASP Top 10 Threats – 3 Marks 2. Mitigation of DDoS Attacks – 2 Marks 3. Protection for Against OWASP APIs Top 10 Threats – 3 Marks 4. Virtual Patching – 2 Marks 5. Bot Management – 2 Marks 6. Zero-Day Attack Mitigation – 1 Mark 7. Protecting Against Data Leakage, Malware and Exploits – 3 Marks 8. Traffic Monitoring and Anomaly Detection – 2 Marks 9. Geo-blocking – 1 Mark 10. Real-Time Threat Intelligence –	Marks will be given based on proposed solution demonstration covering use cases mentioned here Note: *OEM's are expected to prepare for the demo on the use cases in their own lab and StockHolding shall not provide any assistance for the same.*	15	20

	1 Mark			
5	Bidder's technical presentation	• Understanding of the Project requirements – 2 Marks • Bidder's WAAP implementation capabilities and experience - 5 Marks • Approach and Methodology with SLA Management – 3 Marks	5	10

Note:

- The bidder is required to provide documentary evidence for each of the above criteria.
- The technical score will be allotted by StockHolding to each bidder against each section and will be considered final.
- 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 70 marks in the technical evaluation will qualify for the commercial bid evaluation.

Commercial Bid Evaluation (Stage 3)

The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened.

Best Value Bid Determination and Final Evaluation (Stage 4)

A composite score shall be calculated for those bidders whose bids are found to be in order.

The weightage for the composite evaluation is as described below:
a. Technical – 70%
b. Commercial – 30%

For Quality and Cost based Evaluation (QCBS), the following formula will be used for evaluation of the bids

Bn = 0.7 * (Tn/Thigh * 100) + 0.3 * (Cmin/Cb * 100)

Where;
Bn = Overall score of bidder under consideration
Tn = Technical score for the bidder under consideration
Thigh = Highest Technical score achieved against criteria among all eligible bids
Cb = Evaluated Bid Cost (as calculated above) for the bidder under consideration
Cmin = Lowest Evaluated Bid Cost (as calculated above) among the financial proposals under consideration.

The bidder achieving the maximum overall score will be selected for the project. StockHolding reserves the right to negotiate with bidder achieving the maximum overall score.

REQUIREMENT

StockHolding has a number of websites that are published over Internet for various business and administrative purposes. Most of these websites are hosted on premise whereas some are hosted by third parties. Being directly published over Internet, these websites are prone to be affected by various security threats and exploits triggered by the external sources. Existence of vulnerability in any of these websites provides opportunity to attackers to gain access to and launch severe exploits.

To safeguard the StockHolding's Internet facing websites against such threats and cyber-attacks, StockHolding requires a solution that will detect, filter, and block malicious traffic in real time to protect these websites and web applications and protect them from data breaches & defacement. In order to ensure continuous and unfettered access to StockHolding's applications, it is proposed to enable Cloud Based bundled WAF and DDoS protection services on the StockHolding's web applications. This Request for Proposal document ("RFP document" or "RFP") has been prepared solely for enabling the StockHolding to purchase the said services.

Scope of Work

StockHolding is inviting bids for Cloud Based Web Application Firewall and API Security solution for its public facing applications. The proposed solution/model should be a comprehensive and complete Web Application Security Service.

The Successful Bidder will be responsible for supply, installation, maintenance, integration, implementation, support, and management of Cloud-based Web Application Firewall (WAF) and API Security solution with Warranty, AMC, and Technical Support of the solution for a period of 3 years.

Cloud WAF solution should protect the all-configured websites and web services from any kind of application layer attacks covering all OWASP Top 10, & SANS 25 and other known and 0-day attacks including network & application layer DDoS attacks. Cloud WAF and Anti DDOS Solution should be of enterprise grade Web Application and API Protection solution that can accurately detect and mitigate application layer DDoS attacks on websites and web services and secure them from getting compromised. The solution should perform policy-based inspection, signature-based mitigation, AI-based anomaly detection and remediation on incoming HTTP traffic as well as filtering responses for data leak prevention. It should safeguard web applications from getting defaced, compromised and suffer downtime due to malicious activity from attackers 24/7.

A. Task and Deliverables

1) Supply, installation and commissioning of Cloud based WAF and DDOS service with clean bandwidth of 50Mbps/15TB/month. Bidder is responsible for deputing qualified person(s) for installation, configuration, testing and commissioning under the scope of work as per the Technical Specification.

2) All the modules in the proposed solution should be from the same OEM only.
3) The bidder should provide comprehensive technical support services for all the software supplied for the entire period of the contract. Any software/firmware enhancement through update and upgrade released during the contract period by the OEM shall be supplied, installed, and configured without any additional cost to StockHolding.
4) The bidder shall ensure that the supplied Software should work seamlessly with the latest updates of OS Patches /Antivirus Patches in the StockHolding's environment
5) The bidder should provide support to StockHolding as and when required through onsite, remote support, Chat, Phone, email etc.
6) Bidder shall provide detailed professional training during implementation covering installation procedure, configuration, change management process, monitoring and troubleshooting of all software to StockHolding nominated officers. The detailed contents, coverage, venue, and methodology for training will be decided mutually by the bidder and StockHolding.
7) The training shall also cover the following aspects of the systems offered against the tender but not limited to: - training on solution covering fundamentals, device configuration, and performance tuning, troubleshooting etc.
8) The training course shall be structured and imparted by OEM/Bidder personnel only without any additional cost to StockHolding.
9) The bidder shall submit all the necessary technical documents/brochures etc. for the quoted items along with the commercial offer.
10) StockHolding has the right to audit the data center of the OEM where the WAF platform is hosted.
11) Separate tenancy has to be created for this implementation. All supplied Software Licenses should be in the name of StockHolding Corporation of India Limited.
12) Secure Communication Channels:
    a. TLS Encryption: All data exchanged between the SaaS WAF and Stockholding' infrastructure should be encrypted using TLS to prevent interception or tampering.
    b. Mutual TLS (mTLS): Ensures both the WAF and Stockholding' infrastructure authenticate each other to prevent unauthorized entities from joining the communication.
    c. IP Whitelisting: Restrict communication to specific, trusted IP addresses or ranges based on StockHolding's requirements.
13) Traffic Validation
    a. Source Validation: The WAF should ensure incoming traffic is legitimate and not spoofed.
    b. Health Checks: OEM needs to ensure that the WAF platform should perform regular health checks on Stockholding' application url's to validate its readiness and availability for secure communication.
14) API Security (as and when deployed)
    a. Authentication: APIs exposed by the SaaS WAF for integration with the Stockholding' infrastructure should require secure API keys, OAuth tokens, or

other authentication mechanisms.

b. Rate Limiting: Should prevent abuse of APIs by limiting the number of requests from a single source.
c. Input Validation: Should protect against injection attacks by sanitizing all inputs to the APIs.

15) Data Integrity and Validation
   a. Digital Signatures: Ensures data transmitted between the SaaS WAF and the Stockholding' infrastructure has not been tampered with during transit.
   b. Checksum Validation: Verifies the integrity of transmitted files or data.
   c. Secure Logs: Logs of interactions between the SaaS WAF and the Stockholding' application url's are stored securely to detect unauthorized changes or anomalies.

16) Continuous Monitoring and Alerts
   a. Anomaly Detection: WAF should monitor for unusual traffic patterns or activities in the communication between the SaaS WAF and the Stockholding' infrastructure.
   b. Threat Intelligence: WAF should leverage global threat databases to detect known attack signatures in the traffic.
   c. Real-Time Alerts: WAF should notify administrators of potential attacks or suspicious activities.

17) Transitioning from on premise WAF to SaaS based WAF:

17 domains to be considered for migration to Cloud based WAF.

Before Migration:

a. New Attack Surface Introduced: OEM has to take care of these attack surface for mitigation.
b. Man-in-the-Middle (MITM) Attacks: Interception of traffic between the SaaS WAF and Stockholding' infrastructure if not encrypted properly.
c. Service Misconfigurations: Errors during configuration can expose sensitive traffic or services.
d. DNS Dependency: SaaS WAFs often rely on DNS changes to redirect traffic to their infrastructure. DNS setup must be well secured.
e. DNS Security: Use DNSSEC to secure DNS queries.
f. Ensure End-to-End Encryption

During Migration:

a. Testing to Production Environment: Test configurations in a staging environment before going live and later on make it as a production environment.
b. Data Leakage During Migration: Traffic has to be encrypted during migration to avoid exposure of sensitive data.

After Migration:

a. Continuous Monitoring:
   i. Monitor traffic between the SaaS WAF and customer infrastructure for anomalies.
   ii. Use network logs and alerts to identify potential threats.
b. API Security:

i. Secure APIs used by the SaaS WAF with strong authentication mechanisms like OAuth or API keys.

18) Latency Exploitation

To overcome attack scenarios like Timing attacks, Traffic disruptions, Session hijacking and Replay attacks, the following mitigation strategies should be applied as mentioned under;

a. **Traffic Routing and Optimization**:
   i. SaaS WAF OEMs must have geographically distributed Points of Presence (PoPs) to reduce latency.
   ii. Should implement low-latency communication protocols like TLS 1.3

b. **TLS Optimization**:
   i. Use modern protocols like TLS 1.3 to reduce handshake delays.
   ii. Enable session resumption mechanisms such as TLS tickets.

c. **Traffic Prioritization**:
   i. Implement Quality of Service (QoS) policies to prioritize critical application traffic.

d. **Response Time Monitoring**:
   i. Continuously monitor latency and set alerts for anomalies that might indicate an ongoing attack.

e. **Rate Limiting and Session Expiry**:
   i. Limit the number of allowed requests per user/session and enforce short session lifetimes to reduce the risk of session hijacking.

f. **Performance Benchmarks:**
   i. Acceptable latency thresholds for traffic routing through the SaaS WAF (<50ms for most requests).
   ii. periodic performance testing and reporting.

g. **Real-Time Monitoring**:
   i. Provide tools and dashboards that allow Stockholding to monitor response times, traffic patterns, and anomalies.
   ii. OEM should notify Stockholding of latency anomalies that may indicate potential attacks.

h. **Latency Mitigation Controls**:
   i. OEM should implement rate limiting, anomaly detection, and encrypted traffic inspection to mitigate latency-related risks.
   ii. Including automated detection and blocking of replay or timing-based attacks.

19) Assessment & Planning

i. Review current on-premises WAF configurations and identify necessary changes that would be required in a Cloud based WAF.
ii. Identify registrar records (DNS, SSL, etc.) that need to be updated for the cloud-based WAF transition.
iii. Define a timeline and plan for the migration process with minimal downtime.

20) Cloud WAF Configuration

i. Configure security rules, policies, and logging in the cloud WAF.
ii. Existing on-premises WAF configurations and security policies will be evaluated and mapped to the cloud-based solution.

iii. SI and OEM has to ensure correct traffic routing.

21) DNS-Related Changes
   i. Update DNS settings to point to the new cloud-based WAF endpoints.
   ii. Modify A, CNAME, and/or TXT records as required for integration.
   iii. Update domain registrar with new IP addresses for the cloud-based WAF.
   iv. Ensure proper configuration of SSL certificates for encrypted communication.

22) Testing and Validation
   i. Test DNS propagation and ensure proper redirection to the cloud-based WAF.
   ii. Conduct penetration tests and vulnerability assessments on demand basis to verify proper WAF rule enforcement.
   iii. Validate application behaviour, ensuring that there is no disruption to end-users during the migration process.

B. Support

1) One contact number for all support (user/technical) needs would be preferred. Bidder should provide the address and telephone number for the general customer/ technical support location at Mumbai/MMR.
2) Bidder will depute 1 onsite official for 1-month post Go-Live signoff. The duty hours of onsite qualified engineer would be 9.30 AM to 6 PM. In urgent circumstances, bidder will ensure the availability of Onsite Engineer for smooth operations and support services as and when required by StockHolding during the period of contract.
3) Bidder will ensure that deployed solution and all dependencies are under OEM warranty, as applicable, during the period of contract.
4) During period of contract, Bidder will provide support as per resolution matrix defined in this RFP. Non-adherence to resolution matrix will be considered as breach of SLA and dealt as per terms of RFP.
5) Bidder will ensure that at no given point of time during the period of contract the implemented solution or its component are out of OEM warranty/support.
6) The services shall be reviewed as per SLA.

OEM / SI Support

1) The solution should come with 24x7 OEM Support with dedicated account manager and toll free number
2) The solution should show uptime status on GUI and should send monthly uptime reporting via email as and when required
3) The OEM of the proposed solution should be ISO 27001, 14001 and ISO 9001 certified.
4) The OEM of the proposed solution should also provide periodic custom attack summary and conduct configuration efficacy for configured web applications.

Documentation and Deliverables

1) Project Documentation – Solution Architecture, Implementation & Roll-out plan.
2) SOP Document for operating all the solution components.
3) User Manual and/or Training material.

Service Level Agreement (SLA) and Penalty

Implementation SLA and Penalty

Schedule	Timelines	Payment linked to corresponding stage	Penalty
Implementation & Go-Live (sign off) of Saas based WAAP Solution	Within 30 days from the date of acceptance of work order.	Post-sign off	If not implemented within 3 weeks from the date of acceptance of work order, 0.5 % of the Total Solution & Implementation Cost/week subject to maximum of 10% of the Total Solution Cost, will be levied as penalty. Fraction of week shall be construed as one week for the said purpose. Once the maximum is reached, StockHolding reserves the right to cancel the order at its discretion and the Performance Bank Guarantee submitted may be invoked. Documentation Deliverables shall also be completed.
Additional / incremental requirements (for External WAF)	Within 30 days of written communication of the same from StockHolding	Post-sign off	If not implemented within 10 days from the date of receiving the request, 0.5 % of the Total Solution & Implementation Cost/week subject to maximum of 10% of the Total Solution Cost, will be levied as penalty. Fraction of week shall be construed as one week for the said purpose. The said penalty shall be recovered from subsequent year's annual payment. For 3rd year, the penalty amount shall paid by the bidder post which PBG shall be returned

Service level and Penalty

1) The supplier should provide 24*7 Support through Email, Phone and On-Site if required without any additional cost to StockHolding and as and when required by StockHolding.

2) The supplier should integrate new applications with WAF as and when requested by StockHolding, within 7 working days of having raised such a request.
3) Successful bidder shall work with StockHolding's website hosting service provider to diagnose the issues during non-availability of the website services under WAF.
4) Uptime of WAF should be 99.9% on monthly basis. Partial or full unavailability of WAF shall be treated as downtime. StockHolding reserves the right to impart penalty on the Bidder for having an Uptime of less than 99.9% as per the rates given in the table below:

Service Level	Penalty(% of Annual Costs)
99.9% and above	NA
99.9% to 99.5%	5%
99.5% to 99.0%	7%
Less than 99%	10%

5) If there are more than 12 instances of downtime in a year, StockHolding has the right to cancel the contract apart from forfeiting the performance bank guarantee.
6) If there are more than such instances as mentioned in point 5,
7) The uptime will be calculated as per the formula given below:
8) Uptime (%) = (Sum of total hours during month – Sum of downtime hours during month) X 100 / Sum of total hours during month
9) Total hours in a month will be taken as: 24hrs* no. of days in respective month. Any downtime scheduled at StockHolding will not be considered for above calculation.
10) Monthly uptime report is required to be furnished to the StockHolding on quarterly basis.
11) Penalties, subject to maximum of 10% of Total Solution & Implementation Cost in any year, will be deducted from the next due payment or if the maximum penalty limit has been reached, the subsequent penalties will be deducted from the PBG.
12) Penalties for not maintaining the desired service levels in case of resolution of issues raised through mail / telephone. Based on the criticality of the incidents, the bidder will have to resolve the incidents as per the response times for different levels of severity indicated in the table given below. The penalty for non-compliance of the above is as indicated below. The issues will be treated as either critical or non-critical as indicated below:

Level	Criteria	Indicative list of issues	Resolution/ Mitigation Time	Penalty
Critical	The identified issue has material business impact and needs to be resolved immediately. This level would	Issues pertaining to implementation of policies / Solution not being able to prevent zero day attacks and other	• Resolution Time – within 4 hours	Rs.5,000/- for every 1 hours of delay beyond standard time upto a cap of 10% of the PO Value

	typically correspond to issues that result into disruption of most or critical services.	vulnerabilities		
Non-Critical	The identified issues have almost zero impact in terms of business. However, issue needs the attention of bidder and shall be fixed on lesser priority.	Issues in registering tickets on ticketing tool / console of the solution	• Resolution Time – within 24 hours	Rs.5,000/- for every 24 hours of delay beyond standard time upto a cap of 10% of the PO Value

Delivery Timelines

1) All Schedules will be calculated from the T Date, i.e. Date of Acceptance of Purchase Order.
2) External WAF for the applications should be deployed within 30 days of Acceptance of Purchase Order.
3) API Security shall be implemented based on StockHolding's requirement at a future date and mutual agreed timelines & SLA's between StockHolding and bidder.
4) Internal WAF shall be implemented based on StockHolding's requirement at a future date and mutual agreed timelines & SLA's between StockHolding and bidder
5) Separate Purchase Order shall be given for additional FQDN's or Internal WAF Implementation.
6) Additional / incremental requirements on the throughput or data transfer or on-boarding additional FQDN's (External WAF) should also be implemented within 30 days of written communication of the same from StockHolding.

Terms and Conditions

A. Payment:

Sl. No	Milestones	Payment
1.	License Subscription for Cloud based WAF + Support Cost	Yearly 90% payment. Balance 10% - Quarterly advance payment. Last quarter payment will be made at the end of the quarter.
2.	License Subscription for Cloud based API Security Solution + Support Cost	Yearly 90% payment on prorate basis based on Go-Live

		Balance 10% - Quarterly advance payment. Last quarter payment will be made at the end of the quarter.
3.	License Subscription for Cloud based Internal WAF + Support Cost	Yearly 90% payment on prorate basis based on Go-Live Balance 10% - Quarterly advance payment. Last quarter payment will be made at the end of the quarter.
4.	One-time Implementation Cost + Training & Documentation – Cloud based WAF	100% payment (one-time)
5.	One-time Implementation Cost + Training & Documentation – Cloud based API Security Solution	100% payment (one-time)
6.	One-time Implementation Cost + Training & Documentation – Cloud based Internal WAF	100% payment (one-time)
7.	Incremental Cost: (Additional Throughput of 5 Mbps) – (Optional)	100% payment (one-time)
8.	Incremental Cost: (Additional 1 FQDN) – (Optional)	100% payment (one-time)
9.	100 hours/year of Professional Services from OEM – (Optional)	100% payment (one-time)

B. Taxes & levies:

a. Applicable TDS will be deducted (recovered) from the payment(s).
b. Taxes/GST as applicable
c. Applicable Penalty/Penalties may be recovered from payment.
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 is submitted.

Contract Duration

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

Refund of Earnest Money Deposit (EMD)

a. EMD will be refunded through NEFT 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 within 15 days after selection 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% of the Contract Value from scheduled commercial banks as per Annexure - 8. This Bank Guarantee shall be valid up to 60 days beyond the completion of the contract period and claim period shall be valid 12 months beyond the expiry of BG. No payment will be due to the successful bidder based on performance,

until the BG is submitted. A penalty of Rs. 5,000 per day will be imposed on the successful bidder 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.

Stock Holding Corporation of India Limited reserves the right to invoke the BG in the event of non-performance by the successful bidder.

Force Majeure

Neither the 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 endeavor 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 successful Bidder will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory of the successful Bidder.

Sub-Contracting

The selected service provider/ vender shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required under this project.

Non-Disclosure Agreement (NDA)

The successful bidder shall execute Non-Disclosure Agreement (NDA) as per Annexure – 9 (shall be provided to the winning bidder), which contains all the services and terms and conditions of the services to be extended as detailed herein.
The support obligations under the agreement will be of OEM. 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.

Termination Clause

i. StockHolding reserves right to terminate the contract without assigning any reason whatsoever by giving 90 days prior written notice to successful bidder. During the Termination notice period successful bidder must adhere to all the conditions mentioned in the 'Exit Management' clause.
ii. StockHolding reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the

adjustment of pending bills and/or invoking the Performance Bank Guarantee under this contract.

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.		
6	Addresses of Firm/Company		
	a) Head Office		
	b) Local Office in Mumbai(if any)		
7	Authorized Contact person		
	a) Name and Designation		
	b) Telephone number		
	c) E-mail ID		
8	Years of experience in implementation of the WAAP solution in India		
9	**Financial parameters**		
	Business Results (last three years)	Annual Turnover	Net Worth
		(Rs. in Crores)	(Rs. in Crores)
	2021-22		
	2022-23		
	2023-24		
	(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/CA Certificate along with enclosures

Dated this..... Day of 2025

(Signature)
(In the capacity of)

ANNEXURE - 2 – Eligibility Criteria

SI. No	Criteria	Documents to be submitted by Bidder
1	The Bidder should be a registered Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 with experience in providing similar services for past 3 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
2	Bidder should have an average annual turnover of at least ₹ 2.8 Crores per annum for last three financial years (2021-22, 2022-23 and 2023-24). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last three financial years.
3	Bidder should have Positive Net worth (minimum ₹1.05 crores) for all the last 03 (three) audited financial years	Certificate from CA mentioning net worth for the past three financial years.
4	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 2 years from the RFP date.	Self-declaration by the bidder on its Letter Head duly signed by the Authorized Signatory
5	The bidder should be the OEM or partner of the OEM for the proposed WAAP	The bidder should provide Manufacturer's Authorization Letter (MAF). If bidder is OEM itself, MAF not required.
6	The bidder should have at least 03 (three) successful implementations in India of the proposed WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date	Copy of order and/ or completion certificate of work
7	The proposed OEM should have ISO 27000 and/or SOC2 Type2 series certifications	Copy of valid certifications
8	OEM should have WAF services hosted from India Data center only and the WAF Inspection should not happen outside India for traffic generated in India during the entire contract period.	Self-declaration by the bidder on its Letter Head duly signed by the Authorized Signatory
9	OEM's Data Centre shall not be in public cloud i.e. Azure, GCP and AWS	Self-declaration by the bidder on its Letter Head duly signed by the Authorized Signatory
10	Bidder shall have support office in MMR region	Bidder to provide office address along with GST details

Note:

a. All self-certificates shall be duly signed and Stamped by Authorized signatory of the Bidder Firm unless specified otherwise.
b. Bidder response should be complete, Yes/No answer is not acceptable.
c. 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 2025
(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

Sl. No	Parameter	Scores	Min. Scores	Max. Scores
	C. Experience of Bidder & Proposed Solution (70 Marks)			
1	The bidder should have at least 03 (three) successful implementations in India of the WAAP solution of the OEM of which 01 (one) should be in the BFSI sector in the last 03 (three) years as on RFP date	• 3 projects : 10 Marks • 4-5 Projects: 15 marks • More than 5 Projects: 20 Marks	10	20
2	OEM solution must be positioned in the Leaders Quadrant of the latest IDC MarketScape, Gartner Magic Quadrant, or Forrester Wave reports for Web Application Firewall and API Protection.	Presence of OEM Solution in Leader's Quadrant – 10 Marks	0	10
3	Technical Compliance for Solutions	Based on the features mentioned in Annexure-10	30	40
	D. Presentation & Solution Demonstration (30 Marks)			
4	OEM proposed solution Use Cases that needs to be demonstrated during the Demo session are mentioned below: 1. Protection Against OWASP Top 10 Threats – 3 Marks 2. Mitigation of DDoS Attacks – 2 Marks 3. Protection for Against OWASP APIs Top 10 Threats – 3 Marks 4. Virtual Patching – 2 Marks 5. Bot Management – 2 Marks 6. Zero-Day Attack Mitigation – 1 Mark 7. Protecting Against Data Leakage, Malware and Exploits – 3 Marks 8. Traffic Monitoring and Anomaly Detection – 2 Marks 9. Geo-blocking – 1 Mark 10. Real-Time Threat Intelligence – 1 Mark	Marks will be given based on proposed solution demonstration covering use cases mentioned here Note: *OEM's are expected to prepare for the demo on the use cases in their own lab and StockHolding shall not provide any assistance for the same.*	15	20

5	Bidder's technical presentation	• Understanding of the Project requirements – 2 Marks • Bidder's WAAP implementation capabilities and experience - 5 Marks • Approach and Methodology with SLA Management – 3 Marks	5	10

Note:

- The bidder is required to provide documentary evidence for each of the above criteria.
- The technical score will be allotted by StockHolding to each bidder against each section and will be considered final.
- 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 70 marks in the technical evaluation will qualify for the commercial bid evaluation.

ANNEXURE - 4 - Commercial Price Bid Format

Commercial Price Bid Format

Mandatory Components

Sl. No.	Description	Quantity	1st Year Price (₹)	2nd Year Price (₹)	3rd Year Price (₹)
1	License Subscription for Cloud based WAF + Support Cost	01			
2	License Subscription for Cloud based API Security Solution + Support Cost	01			
3	License Subscription for Cloud based Internal WAF + Support Cost	01			
4	**One-time Implementation Cost + Training & Documentation – Cloud based WAF	01		NA	NA
5	**One-time Implementation Cost + Training & Documentation – Cloud based API Security Solution	01		NA	NA
6	**One-time Implementation Cost + Training & Documentation – Cloud based Internal WAF	01		NA	NA
	Total Cost without GST (☐)				
	GST (☐)				
	Total Cost with GST (☐)				
	Grand Total for 3 Years with GST (☐)				

Notes:

a Price to be quoted is for contract period of 03 (three) years including GST while uploading financial bids on GeM portal.

b StockHolding reserves the right to negotiate with L1 bidder.

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.

d All payments will be made in INR.

e **One-time Implementation cost – Amount to be quoted under 1st year price. The cost proposed by the selected bidder will be considered for payment even if the component install on 2nd or 3rd year of the Contract period. And support will be considered from the respective year till the end of the said contract.

Optional Cost Component

Sl. No.	Description	Cost (₹)

1	Incremental Cost: (Additional Throughput of 5 Mbps)	
2	Incremental Cost: (Additional 1 FQDN)	
3	100 hours/year of Professional Services from OEM	
	Total Cost without GST (₹)	
	GST (₹)	
	Total Cost with GST (₹)	

Notes:

a Price to be quoted under 'Optional Cost Component' will not be considered for evaluation. Those components are required on need basis. StockHolding may avail these components during the contract period at the same rate proposed by the selected bidder as part of commercial proposal during the bid submission.

ANNEXURE - 5 – Integrity Pact

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

(_____ 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.) and Smt. Niva Singh, IRAS (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-Contractor"s 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 - Covering Letter on bidder's Letterhead of Integrity Pact

To,

---------- ----------

Sub: RFP REF NO: CPCM-07/2025-26 dated 02-Jul-2025 - Procurement of Cloud based Web Application and API Protection (WAAP) for 03 (three) years for StockHolding

Dear Sir,

DECLARATION

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

Yours faithfully,

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

ANNEXURE – 7 – Compliance Statement

(To be submitted on Company Letter Head)

RFP REF NO: CPCM-07/2025-26 dated 02-Jul-2025 - Procurement of Cloud based Web Application and API Protection (WAAP) for 03 (three) years for StockHolding

DECLARATION

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by StockHolding. We also agree that StockHolding reserves its right to reject the bid, if the bid is not submitted in proper format as per 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)		
5	Non-Disclosure Agreement		
6	Payment Terms		
7	Bid Validity		
8	Integrity Pact		
9	All General & Other Terms & Conditions in the RFP		
10	Requirement		

(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 – 8 – 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 – 9 – 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, 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.
3. **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.

4. **No Warranty**: All Confidential Information is provided 'as is.' Neither Party makes any warranty, express, implied or otherwise, regarding its accuracy, completeness or performance.
5. **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.
6. **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.
7. **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.

8. **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.
9. **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.
10. **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:

ANNEXURE – 10 – Technical Compliance

Sr. No.	Requirements	Compliance Y/N	Evaluation Marks (0 Marks if Compliance = N)
1	**General Features**		
1.1	The Proposed Solution should have capability to support minimum 50000 https https Concurrent Connections.		2
1.2	Proposed Solution must be a SaaS offering for WAAP (web application & api protection) along with DDOS (L3/L4 and L7) with client side defense & Bot Defense from single platform		2
1.3	The proposed solution must support policy nesting at layer7. The proposed solution must support policy nesting at layer7 to address the complex application integration		2
2	**SSL/TLS Handling**		
2.1	The proposed solution should facilitate SSL handling.		2
2.2	The system must be able to establish SSL session before sending any packet to backend servers		2
2.3	The system must support elliptic curve cryptography (ECC)		2
2.4	The system must support SSL/TLS client certificate authentication		2
2.5	The system should support TLS v1.1, v1.2, TLS v1.3, SSL v2 & SSL v3 (Highest version available)		2
2.6	Proposed solution should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for each application service		2
2.7	The system must store the certificate private key using a secure mechanism (With & without passphrase)		2
2.8	The system must capable of communication with the original backend application server / Application service over SSL or TLS. should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for the SSL/TLS connection to the backend server		2
3	**Web Application Firewall**		
3.1	The solution should address and mitigate the OWASP Top 10 web application/ mobile application security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability is addressed by the solution).		2
3.2	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions to address the compliances and configure policies for it.		2
3.3	When deployed as a full proxy mode, the Web application firewall should be able to digitally sign cookies, encrypt cookies, and to rewrite URLs		1

3.4	The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures) . The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats		2
3.5	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage. Should provide facility to configure time for staging of policy and policy should move to blocking once staging time is over.		2
3.6	The solution must support virtual patching for known vulnerabilities without requiring changes to application code.		2
3.7	The solution must be able to validate encoded data in the HTTP traffic		2
3.8	The solution must be able to identify Web Socket connections and provide security for WebSocket including security for exploit against Server abuse, login enforcement, XSS and SQL injection. The Solution must be able to parse and monitor JSON data over web socket protocol		2
3.9	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.		2
3.10	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode.		1
3.11	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.		1
3.12	The Proposed Solution should have capability to mitigate, learn and adapt to unique application layer user interaction patterns to enable dynamic defenses based on changing conditions		2
3.13	The Proposed Solution should have Correlated Attack Validation capability or Correlation features which examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks and also to eliminate false positives.		2
3.14	The Proposed WAF Solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.		2
3.15	Proposed solution should have capability to block Brute force attack traffic		2
3.16	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks		2

3.17	Proposed Solution should have ability to automatically detect application platform and its technology used on backend side to define signature sets required for defined Proposed Solution policy.		1
3.18	Proposed Solution should have ability to configure way to analyze request payload based on custom rules for each URL entry configured in the security policy		2
3.19	Proposed Solution should be able to track application changes over time and adjust config elements and rules based on that data.		2
3.20	The WAF instance should have option to enable x-forwarder option per service to log actual client IP in webserver logs even deployed in Reverse Proxy mode.		2
3.21	Proposed WAF Solution should have functionality to showcase how many URLs in the application have been completely learned & move them into Protection Mode automatically i.e. some URLs to be in learning mode & some URLs in the Protection Mode of the same Application		1
3.22	Proposed WAF Solution should have capability to learn changes in the already integrated Web Application & protect it at the same time i.e. solution should be able to learn changes in the application in the Protection Mode. Proposed Solution should have option to learn policy and configure the application in block mode simultaneously		1
3.23	The WAF Solution should have ability to configure application in block mode partially and learn the traffic for filters whose fine tuning is yet to be configured		1
3.24	Should be able to uniquely detect and block if required the end user on the basis of internal IP address, Plugins Installed in the browser, OS, Screen Resolution, Fonts etc. instead of going with traditional IP based blocking only		1
3.25	Solution should dynamically understand the Changes on the Web/Application Server		1
3.26	Should provide Policy creation per URL and not generic policy for URL's		2

3.27	System should protects against the following threats/attacks: • SQL injection • Cross-site scripting (XSS) • Cross-Site-Request-Forgery (CSRF) • Parameter tampering • Hidden-field manipulation • Session manipulation • Cookie poisoning • Stealth commanding • Backdoor and debug options • Application-buffer-overflow attacks • Brute-force attacks • Data encoding • Unauthorized navigation • SOAP- and Web-services manipulation • Web Scraping • Directory/Path traversal • Remote File Inclusion		2
3.28	System supports enforcing policies regardless of character encoding in order to combat evasion techniques, WAF should support Policy Evasion Detection Engine to combat evasion techniques such as: • URL-decoding (for example, %XX) • Self-referencing paths (that is,. use of /./ and encoded equivalents) • Path back-references (that is, use of /../ and encoded equivalents) • Mixed case • Excessive use of whitespace • Comment removal (for example, convert DELETE/**/FROM to DELETE FROM) • Conversion of (Windows-supported) backslash characters into forward slash characters. • Conversion of IIS-specific Unicode encoding (%uXXYY) • IIS extended Unicode • Virtual directory route—positive folder enforcement • Base64 Encoded parameters & headers		1

3.29	The solution must provide the following features and protection: a. HTTP protocol validation b. Correlated based attack protection c. HTTP protocol attack signatures d. Cookie signing validation e. Anti-website scraping f. Whitelisting based protection g. Web worm protection h. Web application attack signatures i. Web application layer customized protection		2
3.3	The proposed WAF should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection f. Form Field and Parameter Tampering and HPP attacks g. Sensitive information leakage h. Session highjacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling p. Parser protection (XML Bombs, Recursion Attacks)		2
3.31	WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, Converting back slash to forward slash character etc.		1
3.32	Should support XML Applications - solution must be able to protect web applications that include Web services (XML) content.		2
3.33	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.		2
3.34	The proposed WAF should provide application-specific XML filtering and validation functions that ensure the XML input of web-based applications is properly structured. It should provide schema validation, common attacks mitigation, and XML parser denial-of-service prevention.		2
3.35	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for set amount of time (Tarpit action)		1
3.36	The system must capable of blocking specific list of HTTP methods		2

3.37	The system must be able to allow or disallow specific file type		2
3.38	The system must be able to enforce specific HTTP headers and values to be present in client requests		2
3.39	The system must be able to perform information display masking/scrubbing on requests and responses		2
3.4	The solution must be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user d. Block the IP address		1
3.41	The solution must be able to block the user or the IP address for a configurable period of time		1
3.42	The solution must be able to send a TCP RST packet to both ends of a web connection when it is deployed in sniffing mode in the event of active enforcement deployment mode		1
3.43	The solution must be able to protect both HTTP Web applications, SSL (HTTPS) web applications & Should support HTTP/2.		2
3.44	The solution must be able to decrypt SSL web traffic between clients and web servers		2
3.45	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode		2
3.46	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection		1
3.47	The solution must include a pre-configured list of comprehensive and accurate web attack signatures		2
3.48	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications		2
3.49	The solution must provide signature protection against known Vulnerabilities in commercial infrastructure software such as Apache, IIS and so on. The content provided by the signature detection mechanism must be based on the research done by the solution vendor threat intelligence division and a combination of other resources such as Snort, CVE and so on. This set of signatures must have an option to be continuously and automatically updated		2
3.50	The solution must support regular expressions for the following purposes: a. Signatures definition b. Sensitive data definition c. Parameter type definition d. Host names and URL prefixes definition e. Fine tuning of parameters that are dynamically learnt from the web application profiles		1
3.51	The solution's in-built correlation engine must address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol and		1

	application levels over time to distinguish between attacks and valid user traffic		
3.52	The solution must inspect and monitor all HTTP(S) data and the application level including HTTP requests and responses, HTTP(S) headers, form fields, and the HTTP(S) body		2
3.53	The solution must be able to inject HTML snippet/text in the HTTP response		2
3.54	The solution must automatically discover HTTP traffic content type, regardless of the content-type HTTP header. With this capability, WAF should be able to parse and protect HTTP Requests with missing or wrong content-type header		2
3.55	The solution should protect against Deserialization attacks, accomplished by searching for signatures in the 'Request-Content' header		1
3.56	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.		2
3.57	The solution must be capable to automatically create whitelisting/profiling of web applications.		1
3.58	The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria.		2
3.59	The solution must be able to perform virtual patching for its protected web applications.		1
3.6	The solution must support the capability to define security policies based on the threat intelligence feeds listed previously to perform the following functions: a. Alert b. Block IP c. Block Session d. Block User		2
3.61	The proposed Solution should be session aware and should be able to enforce and report session		2
3.62	The solution must be able to track and monitor web application users. This user tracking mechanism must be automated, with no changes to the existing application or authentication scheme.		1
3.63	The proposed Solution should be able to protect against Manipulation of invalidated input		1
3.64	The proposed Solution should protect against requests for restricted object and file types		1
3.65	The proposed Solution should support Device Fingerprint technology by involving various tools and methodologies to gather IP agnostic information about the source. Fingerprint information should include the Client Operating System, browser, fonts, screen resolution, and plugins etc.		1
3.66	The proposed Solution should conceal any HTTP error messages from users		2

3.67	The proposed Solution should remove application error messages from pages sent to users		2
3.68	The proposed Solution should prevent leakage of server code		2
3.69	The proposed Solution should support XPATH injection		2
3.7	The proposed Solution should support RSS/Atom feed injection		2
3.71	The proposed Solution should support RSS/Atom feed injection		1
3.72	Geo-location-based IP blocking to be supported by Web Application Firewalls (WAFs) to allow administrators to block or allow traffic from specific geographic locations (i.e., countries, regions, or continents) based on the IP address of the incoming request. be particularly useful for mitigating attacks that are originating from regions with little or no business relevance or from areas known for high levels of malicious activity.		2
4	**Automated threat attacks/BOT Attacks/Application DDOS - Protection, Detection & mitigation**		
4.1	Proposed Solution should protect against OWASP Top-20 Automated threats for Applications		2
4.2	The proposed solution should have the capability to proactively identify bots		2
4.3	The solution should be 100% automated and should not require bot-specific resource (from the organization) to manage the solution.		2
4.4	The Solution have below flexible attack mitigation options, a. Blocking of User/session b. Feed Fake Data to Bots c. Captcha Challenge d. Filter the traffic. e. Throttle/Rate based Blocking. f. Session termination g. Redirect loop to the Bad Bot h. Custom business logic		2
4.5	The Solution must be able to Detect below types of Bad Bots: a. Misbehaving Legitimate Bots b. Bot Attacking from Public Cloud c. Known bad Bots d. Scripted Bots e. Programmatic session behavior. f. Advance Java Script validation Failure g. Malicious Browser Behavior h. Emulator tools i. Low and Slow Attacks j. Malicious intent detections		2
4.6	The Solution must be based on Intent oriented and User behavior Oriented		2

4.7	The Solution must able to detect below type of attacks created by Bad Bots. a. Account take over b. Web Scrapping c. Application DDoS e. Form Spam f. API Abuse		2
4.8	The solution must have below Attack Detection and mitigation Mechanism as Core Feature. a. Collective Bot Intelligence b. IP reputation to track proxy and TOR Request c. Semi Supervised machine learning to identify emerging Bot Patterns. d. User behavior analysis for anomaly detection e. Dynamic reverse tuning test to uncover bot identity f. unique device fingerprinting creation h. Global Deception network		2
4.9	The system must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such that: a. Slowloris b. Slow Post d. HTTP GET/POST Flood		2
4.10	The proposed solution should protect against Ability to allow only specific HTTP Methods.		2
4.11	System should support integration with DDOS Solution to mitigate attacks from Mega Proxies HTTP dynamic flood		2
4.12	The Proposed WAF Solution should have option to signal DDoS Solution to block attacker from multiple repeated attempts		2
4.13	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests		2
4.14	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript, Image and Sound CAPTCHA challenges. This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot.		2
4.15	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behavior analysis, reverse DNS lookup		2
4.16	The Web Application Firewall should have "Anti-Automation" protection which can block the automated attacks using hacking tools, scripts, frame work etc.		2
4.17	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It		2

	should have CAPTCHA support or other mechanism to avoid distributed attack.		
4.18	Solution should support Behavioral L7 DDoS mitigation to detect attacks without human intervention.		2
4.19	Proposed WAF Solution should be able to provide a threat intelligence feed and service for bots protection & should be able to carry out Bot Classification of traffic into humans, Trusted Bot, Bad Bot, General Bot and Unknown new bot - Bot Type: Click Bot, Comment Spammer Bot, Crawler, Feed Fetcher, Hacking Tool, Masking Proxy, Search Bot, Spam Bot, Vulnerability Scanner, Worm, Site Helper and DDoS Tool		2
5	**API Security**		
5.1	The solution should address and mitigate the OWASP Top 10 API security vulnerabilities		2
5.2	Solution should have multiple methods for Securing API Communication including the OpenAPI/Swagger Integration		2
5.3	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.		2
6	**Monitoring, Logging & Reporting**		
6.1	Proposed solution should have the detailed Access logs, Change logs for audit trail purpose		2
6.2	The system must provide built in logging to 3rd party security event tracking systems such as SIEM like Arcsight, Splunk, Remote Syslog, IPFIX, QRadar etc.		2
6.3	The solution should also support sending of logs in CEF (Common Event Format) standard		2
6.4	There should be centralized Monitoring and Management station with capability for log collection for minimum 180 days		2
6.5	The system must provide request logging that support profile by enabling configuration log entries to be reported when requests/responses are received, supports audit logging of HTTP/decrypted HTTPS requests/responses, and enables specification of a response to be issued when a specific requests/responses occur.		2
6.6	The system shall have ability to generate service and system statistics. Provides dashboard displays anomaly statistics about number attacks, dropped requests, a summary of system traffic.		2
6.7	The system must provide high-level view of recent activity in a single screen, where you can view aggregated events (incidents) rather than individual transactions (that are displayed on the Requests screen). Incidents are suspected attacks on the application.		2
6.8	The proposed solution should have the capability to capture tcpdump, packet capture for forensic analysis.		2

6.9	The solution must provide pre-packaged reporting capabilities out-of-the-box without user intervention/further configuration: a. Alert analysis (For Application user, Known attack patterns, severity, Source IP with severity & type, URL, User with severity & type, Violation Types) b. Daily & weekly Top 10 WAF violations c. Daily Summary Blocked Connections d. Data Leakage Report e. Directory Browsing Detection Report f. List of Alerts g. PCI - WAF violations h. Sensitive Error Messages Leakage Report i. Slow HTTP/S Alerts		2
6.10	The solution must have the functionality within the UI out-of-the-box that enables the administrator to create custom report templates based on the existing out-of-the-box reports.		2
6.11	The solution must support automatic generation of reports based on a defined schedule.		1
7	**Administration**		
7.1	Proposed Solution should have Role-based management & Access Control along with Multi-Factor Authentication (MFA) based user authentication. Proposed Solution should be able to define different roles and associate appropriate access levels. The Proposed SaaS Based WAAP solution should support unlimited management user accounts		2
7.2	Proposed solution should have Web GUI (HTTPS) for management. The solution must allow the user to use a standard browser to access the management UI		2
7.3	Proposed solution should have the capability to restrict Web GUI from specific IP address		1
7.4	The entire solution must be centrally managed for day to day operations. Reporting, policy creation, alerts management, web application protection configuration, etc must be managed from the management server.		2
7.5	The solution must support the following password management capabilities and lockout facilities without relying on any external system		1
8	**(East-West Traffic) Internal Web Application Firewall (WAF)**		
8.1	Traffic Monitoring & Inspection - Inspects both inbound and outbound traffic at the application layer to detect threats like SQL injection, cross-site scripting (XSS), and other common vulnerabilities.		1
8.2	The WAF should seamlessly integrate with microservices-based architectures, inspecting traffic between containers, APIs, and services.		1
8.3	Restrict internal service access based on the identity of users, services, or containers. For example, an internal service may only communicate with specific other services, and the WAF can enforce these rules. Policies can be based on application-layer context, like the nature of the request, service type, or even user roles within the internal system.		1

8.4	Behavioural Analytics - Monitors for unusual patterns in traffic, such as unexpected spikes or traffic to internal endpoints that typically do not get much access.		1
8.5	End-to-End Encryption: Ensures that data remains encrypted between services, with the ability to decrypt and inspect traffic if necessary for security purposes.		1
8.6	SSL/TLS Termination: Supports SSL/TLS offloading or end-to-end encryption inspection to detect threats even in encrypted traffic.		1
8.7	Rate Limiting: Detects and limits excessive requests from internal services that may be attempting to overwhelm a resource or conduct a DoS/DDoS attack.		1
8.8	Bot Detection: Identifies and blocks internal traffic originating from automated bots or compromised services.		1
8.9	Self-Learning Mechanism: The WAF should adjust security policies dynamically based on the analysis of traffic, evolving security threats, and service-specific risk profiles.		1
8.10	Seamless integration with Security Information and Event Management (SIEM) systems, vulnerability scanners, and other monitoring tools.		1
8.11	The WAF should not introduce significant latency in traffic flow, especially in microservices environments where performance is crucial.		1
8.12	Capable of handling high volumes of internal traffic without impacting the performance of services.		1
8.13	The WAF should be deployed in a highly available manner with redundancy to ensure consistent protection even in the case of failures or downtime.		1
8.14	Provides a user-friendly interface for configuring policies, monitoring traffic, and reviewing reports.		1
81.5	Hybrid: Should have a Combination of inline and out-of-band modes, offering a balance of security and performance.		1
8.16	Setup for East-West WAF shall be installed on a Virtual Machine at StockHolding premises. VM's shall be provided by StockHolding		1