RFP For Procurement of WAF System

Request for Proposal (RFP)

For

RFP For Procurement of WAF System for SSL Setup

StockHolding Services Ltd.

P-51, SHCIL House, Mahape, MIDC Navi

Mumbai - 400 710

RFP For Procurement of WAF System

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 STOCKHOLDING Services Limited (SSL), 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 *SSL* 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. *SSL* 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. *SSL* may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

RFP For Procurement of WAF System

Document Details

Name of the Company	StockHolding Services Ltd	
RFP Reference No	RFP/SSL/ITSER/2026-27/003	
Date of issue	3rd June 2026	
Schedule for Receipt of Bids	Date	12th June 2026
	Time	03.30 P.M.
Schedule for Opening of Bids	Date	12th June 2026
	Time	4.30 P.M.
Place of Pre-bid meeting/ Submission and Opening of Bids / address for Communication & Contact person	**Stockholding Services Limited** SHCIL House, P-51, TTC Industrial Area, Mahape, Navi Mumbai Pin 400710. **Name: Shivani Narkhede** **Tel. No. : 022- 61778649** **Email ID : IT_Tender@Stockholdingservices.com**	
For Technical Queries	**NAME: Shivani Narkhede** Tel. No. **: 022- 61778649** Email ID: **IT_Tender@Stockholdingservices.com**	
E-bidding to be facilitated by	GeM Portal	
Address for online submission of bids	Bid must be submitted online on Https://gem.gov.in	
This bid document is not transferable		
GEM ID : **BID NO:** GEM/2026/B/7617465		

RFP For Procurement of WAF System

Table of Contents

Overview – About STOCKHOLDING Services Limited (SSL)

SSL is a broking arm of Stockholding Corporation of India Ltd. SSL offers stock broking services and is also into distribution of various third party financial investment products and services SSL has its registered office at Navi Mumbai.

Objective of the RFP

Objective of this RFP is to procure WAF security service for SSL Infrastructure setup. Detail scope of work is as per Annexure- B.

Submission of Proposal:

The response to this RFP will be submitted by way of two stages bidding process. The Eligibility Criteria with Technical proposal with the relevant information / documents / acceptance of all terms and conditions as described in this RFP document will be submitted to online Tender platform and commercial proposal item/material wise.

In this scenario, if bidder fulfilled all terms mentioned in Eligibility Criteria then only next Technical Criteria will be considered. If Bidder didn't comply with Eligibility Criteria then the said bidder will not be consider for further evaluation and bid from the said bidder will be cancelled. If bidder comply with Eligibility and qualify 70% of Technical Criteria then bidder will consider for commercial evaluation.

The bidders are requested to note that they cannot make their online submission after the time stipulated above and no extension of time will normally be permitted for submission of bid.

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 *SSL* in this regard will be final and conclusive and binding.

Clarifications regarding RFP Document:

- 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 *SSL* for necessary clarifications.
- *SSL* shall not be responsible for any external agency delays.
- *SSL* reserves the sole right for carrying out any amendments / modifications / changes in the bidding process including any addendum to this entire RFP
- At any time before the deadline for submission of bids / offers, *SSL* may, for any reason whatsoever, whether at its own initiative or in response to a clarification requested by bidders, modify this RFP Document.
- It may be noted that notice regarding corrigendum /addendums /amendments/ response to bidders' queries, etc., will be published on SSL's website only. Prospective bidders shall regularly visit SSL's same website for any changes/development in relation to this RFP.
- *SSL* reserves the rights to extend the deadline for the submission of bids, if required. However, no request from the bidders for extending the deadline for submission of bids, shall be binding on *SSL*.
- SSL reserves the right to reject any or all the responses to RFPs / Bids received in response to this RFP at any stage without assigning any reason whatsoever and without being liable for any loss/injury that Bidder might suffer due to such reason. The decision of SSL shall be final, conclusive and binding an all the parties directly or indirectly connected with the bidding process.

Clarification Regarding Extension of RFP and Number of Bids

- SSL is required minimum 3 nos. of proposals for the said RFP process.
- If within a timeline of submission, SSL is not getting 3 Bids, then SSL will extend the bid submission for one time with extension of 3 days.
- After extension of period of 3 days if SSL is not getting 3 bids then SSL will go with qualified bids received in response.
- SSL completely reserved the rights to modify / cancel of the bids at any time. There should not any objection of any bidder and Bidder has to provide confirmation letter of all terms conditions acceptance with the bid documents.

Requirement details with Terms & Conditions

(1) Eligibility Criteria:

Only those Bidders who fulfill the following criteria are eligible to respond to the RFP. Document/s in support of all eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the bidders who do not fulfill any of the following eligibility

criteria are liable to be rejected. **Criteria (Documents to be submitted online along with Technical Bid)**

Evaluation of Offers

Stage 1: Eligibility Criteria (Pre-Qualification) (Stage 1)

1. Each of the conditions for Vendor Compliance and Pre-Qualification criteria outlined in the RFP document must be met by the bidder.
2. Only vendors fulfilling all Pre-Qualification conditions will proceed to the next stage of evaluation.

Stage 2: Technical Evaluation (Stage 2)

1. Technical Evaluation (TE) will be conducted for vendors who successfully meet the Pre-Qualification requirements in Stage 1.
2. Each Technical Bid will be scored out of a maximum of 100 marks, based on the evaluation framework.
3. Vendors achieving a minimum technical score of 70% (70 marks) or more will qualify for the next stage of evaluation.

Stage 3: Financial Evaluation (Stage 3)

1. Financial Evaluation will be carried out only for vendors who qualify through Stage 2.
2. The financial proposal will be evaluated to identify the most cost-effective and value-driven solution.

Eligibility Criteria Pre-Qualification (Stage 1)

Sr. No.	Eligibility Criteria	Documents to be submitted by Bidder /OEM	Complied (Yes/No)
1	The bidder must be registered as a company under the Company Act 1956/2013 or LLP Act 2008 in Thane / Mumbai / Navi Mumbai and should have been in existence for the last 5 years from the issuance date of RFP.	Certificate of Incorporation, GSTIN Certificate,	
2	The bidder should have an average annual turnover of Rs. 01 Crore for the last 3 financial years (2022-23, 2023-24 and 2024-25). Individual company turnover only.	CA certificate & audited financial statements (Balance Sheet & Profit & Loss Statements).	
3	The bidder should have a positive net worth for the last 3 financial years (2022-23, 2023-24 and 2024-25).	CA certificate & audited financial statements (Balance Sheet & Profit & Loss Statements).	

4	The bidder should not have been blacklisted, debarred, or banned at the time of submission by any government organization, statutory body, or BFSI institution.	Self-Declaration on bidder's letterhead duly signed and stamped by the Authorized Signatory.	
5	OEM should have OEM TAC in India (since last 10 years).	Valid Certificate by OEM	
6	OEM must have at least 3 successful implementation.	Self Declaration by OEM on its Letter Head with clients detail Name, Contact person Name, Contact Number and Email Id	
7	OEM should have multiple Cloud WAF PoP & Cloud DDoS Scrubbing Centre in India	Self Declaration by OEM on its Letter Head	
8	OEM should be present in India for More than 20 Years.	Valid Certificate	
9	OEM should have it's own Emergency Response Team located in India	Escalation Matrix on OEM	
10	OEM should be recognised Leaders or strong performer category consecutively in last 2 years by analyst like Spark Matrix Quadrant, Kupingercole, Gigaom	Valid Certificate / Document	

Technical Criteria and Service Requirement:

Cloud Application Security			
Sr No	**Technical Specifications**	**Scores**	**Compliance (Yes / No)**
	OEM Eligibility Criteria		
1	OEM should have OEM TAC in India (since last 10 years).	1	
2	OEM must have at least 3 successful implementation.	1	
3	OEM should have multiple Cloud WAF PoP & Cloud DDoS Scrubbing Centre in India	1	
4	OEM should be present in India for More than 20 Years.	2	
5	OEM should have it's own Emergency Response Team located in India	1	
6	OEM should be recognised Leaders or stron performer category consecutively in last 2 years by analyst like Spark Matrix Quadrant, Kupingercole, Gigaom	2	
	Cloud WAF Technical Specifications :		
1	The proposed Cloud Application Security Service should support **10 Applications** and provide **10 Mbps** HTTP/S traffic from day 1 (Committed at any given point of Time).		

2	Web application attack mitigation covering OWASP Top-10, protecting against Common Web attacks, Data and Access Centric attacks, and Zero Day attacks. Negative and Positive security models, Behavioral Network and Application Layer DDoS Protection with network challenge-response.	1	
3	The proposed service must include DDoS protection up to 10 Gbps of attack traffic.	1	
4	Cloud Cloud WAF, API Protection, BOT Protection, DDoS service should be from the Same Technology OEM. The Cloud Services (Cloud WAF, API Protection, BOT Protection, DDoS) should be provided direclty by the Parent OEM and not by 3rd party Cloud resseller / hosting provider.	2	
5	The proposed service should be Always-On service i.e. all the HTTP / HTTPs Traffic shall be routed to the Cloud PoP through DNS Diversion. Once the Traffic Inspection & Attack Mitigation is done, the Legitimate / Genuine traffic is routed to the respected Origin Server.	1	
6	The service should be comprehensive and include Configuration, Operations and Management of the solution and should be fully managed by Cloud AppSec Provider.	1	
7	No separate Hardware & Software is to be installed at Datacenter Origin Web server for the provision of the Cloud services.	1	
8	The proposed solution should support various features like Application Protection (OWASP TOP 10), Security, Behavioural based DDoS Protection, Geo location based blocking.	1	
9	The Cloud Cloud WAF should provide application protection including OWASP TOP - 10 coverage, advanced attack protection and zero-day attack protection by implementing both negative and positive security model.	1	
10	The proposed solution must provide end to end to protection for Web, Mobile & API.	1	
11	It should be able to prevent all application security threats including Cross Site Scripting (XSS), SQL injection, remote file inclusion, Brute Force Attack, Buffer overflow, Cookie poisoning & Cookie Protection and Parameter tampering.	1	
12	The should have Continuous adaptive policy feature that automatically map applications, detect changes and dynamically deploy the optimal security policy for the application.	1	
13	The Cloud WAF should have machine-learning algorithms to identify legitimate application behavior and perform false-positive correction. Advanced machine-learning algorithms should automatically, and continuously, review large log files, find anomalies and automatically suggest policy refinements.	1	
14	The solution should provide full support for HTML5, AJAX and JSON.	1	
15	The Cloud WAF should be capable of decrypting the SSL/TLS traffic to analyze the HTTP data, and re-encrypt the SSL/TLS traffic.	1	
16	OEM should have support for Cloud DDoS Protection Add-on Service for application protected by the Cloud WAF service. Unlimited DDoS	1	

	attack traffic capacity. Unlimited number of attacks per month. Unlimited duration of attacks per month.		
17	Cloud WAF should have multiple methods for Securing API Communication including the OpenAPI/Swagger Integration feature of API and should support schema upload	1	
18	Should provide Service Level Commitment of 99.999% at least with Service Credits	2	
19	Cloud WAF should have capability to Load Balance & Failover across Origins (DC-DR).		
20	Cloud WAF platform should have capability to Protect Application with Custom Ports. The proposed solution should have an ability to support HTTP/HTTPS traffic delivery and inspection using a non-standard ports range between 1024 and 65534	2	
21	Solution should be able to protect applications regardless the presence of origin server i.e.the origin server can be present in public cloud, private cloud or on-premise datacentres.	1	
22	Should have ability to perform load balancing between different origin IP address in either Active-Active mode or Active-Standby mode.	1	
23	Should be able to protect from DDoS Attacks.	1	
24	It should Allow to configure a custom security page to be displayed to visitors who are violating the web application and API Protection security modules.	1	
25	Cloud WAF and DDoS should be from same OEM so that there is a tight integration between both in terms of integration and security. There should not be separate traffic redirection to be configured by the User.	2	
26	**DDoS Protection add-on for Cloud WAF should support the following :** Behavioral network layer DDoS protection Behavioral application layer DDoS protection Slow rate attacks Network Challenge Response HTTP Challenge Response Access List Weekly Security Update Subscription 10 Gbps Attack volume handling capacity from Day1 and scalable to Unlimited Option.	2	
27	Cloud WAF should allow to address false positives of application-level attacks in a simple, self-service action, through the Cloud portal.	1	
28	The propsed Technology OEM should have Global DDoS Scrubbing Capacity of around 30 Tbps.	2	
29	Solution provider should have local Scrubbing centre (INDIA) to mitigate DDoS Attack. Traffic should not go outside India.	1	
30	Solution should offer feature to control SSL/TLS Version via Cloud Cloud WAF. It should have support for SSL/TSL Version such as SSLv3, TLS 1.0, TLS1.1, TLS 1.2 & TLS 1.3.	1	

31	The proposed solution should support ERT Active Attackers Feed (EAAF) which should have the ability to automatically block low-reputation attackers identified by OEM's Global Deception Network.	2	
32	OWASP protection coverage : Wider protection out of the box and additional security policies optimization per app with its OEM ERT services	1	
33	CONTINUOUSLY ADAPTIVE SECURITY POLICIES: The proposed Service must offer dynamic security policies which learn traffic baselines automatically adapt to each individual application and its unique pattern of user traffic.	1	
34	ZERO-DAY ATTACK PROTECTION: Complete protection with a 'positive' security model, providing protection against zero-day attacks on web application and APIs.	1	
35	BEHAVIORAL DDoS PROTECTION: The proposed Service must offer behavior-based DDoS protection that is not based on rate limits, allowing for better detection, superior protection and fewer false positives.	1	
36	ATTACK-TIME PROTECTION: OEM must provide built-in attack-time support through Emergency Response Team (ERT).	1	
37	POSITIVE SECURITY MODEL: Solution must offer complete protection out-of-the-box with a 'positive' security model, blocking all traffic that does not conform to legitimate user traffic baselines	1	
38	DATA LEAKAGE PREVENTION: Solution must include data leakage prevention (DLP) functionality by outbound masking of sensitive private user data like credit card numbers and SSNs.	1	
39	The proposed solution should have an ability to temporarily block source IP from any activity as a penalty for continuous security violations.	1	
40	The proposed solution should provide AI/ML based "security policy refinement" recommendation service which detects potential false positives and allows for policy refinements to be applied using a self-service portal.	1	
41	The proposed solution should support multi-cloud and hybrid cloud environments leveraging an API-based out-of-path architecture to minimize interruption and impact.	2	
42	The Service should also have the provision for capacity Add-Ons of 10, 50, 100 Mbps and so on.	1	
43	The Service should also have the provision for application Add-Ons of 5, 10 and so on.	1	
44	The service capacity provided should be as per requirement given in commercial bid and no restrictions on data transfer. The same can be upgraded to higher capacity at the contracted rate during the period of contract.	1	
45	The solutions provided must have SIEM integration capability and Cloud based service for pulling Security events in Customer's SIEM Tool (on premise or cloud based).	1	
46	The Service Provider shall provide APIs for pulling security events information in near real time basis from Cloud Service.	1	

47	WAF should support different policies for different web applications and allow modification of these policies upon request.	1	
48	The WAF should allow for exception handling like Whitelisting and Blacklisting of IPs and allow blocking of IPs based on geographic location.	1	
49	Solution should provide browser-side security to ensure the protection against attacks such as form jacking, Magecart (skimming) & supply chain exploits.	1	
50	Solution should have data leakage protection capability by blocking untrusted destinations, parameters & DOM-based XSS	1	
51	Solution should be able to stop any malcious scripts & services without blocking legitimate activity.	1	
52	Solution should have capability to block malicious domain and allow legitimate domains with exception	1	
53	The solution shall support a minimum log retention period of 60 days in compliance with regulatory requirements.	1	
	Cloud BOT Management Technical Specifications :		
1	Identify the intent of bots with the highest precision through semi supervised machine learning models including deep behavioural analysis. SECURE ALL CHANNELS: WEB & MOBILE APPS, APIs - Defend against bots that target various digital assets — even sophisticated bots designed to hit multiple assets.	1	
2	The proposed Cloud WAAP Solution should support the mobile application security to prevent attackers from taking advantage of end users and from carrying out distributed attacks on mobile applications.	1	
3	**Key BOTM Technical Features :**		
a	**Easy Integration** —Flexible deployment options include integration via JS tag, cloud connectors or web server plug-ins. API-based approach should be supported i.e. Domain Name System (DNS) redirection should not be mandatory.	1	
4	Solution should support Detection and blocking of bots in real time with no impact on the technology stack.	1	
	Cloud API Protection Technical Specifications :		
1	**COMPREHENSIVE :** Should protect all the parts of API (header, body, query parameters, methods) against a broad scope of API threats, including data leakage, denial of service, automated threats (bots), embedded attacks, etc.	1	
2	**STATE-OF-THE-ART PROTECTION :** Accurate auto-policy generation based on both positive and negative security models, which continuously optimizes and eliminates false positives. a) Automated security policy generation based on both positive and negative security models b) Ongoing automatic security policy optimization, continuously reducing false positives c) Reporting and analytics to provide insight into documented OpenAPIs, attack reporting dashboard	1	

3	**CONSISTENT SECURITY :** The same security technology engine and policies applied across any environment and architecture – monolithic apps, microservices and serverless.	1	
4	**EMBEDDED ATTACK PROTECTION :** Should detect and block embedded known types of attacks in the API parameters, including injections, deserialization attacks, JSON exploits, XML bombs etc.	1	
5	**SECURITY POLICY SELF-OPTIMIZATION :** Machine-learning based security algorithm that automatically suggests and applies security policy adjustments to correct and eliminate false positives.	1	
6	**API PROTECTION AGAINST AUTOMATED THREATS :** Machine-learning algorithms to detect malicious bot activities targeting APIs from automated attacks such as account takeover attacks (token cracking, credential staffing, account creation), content scraping and data harvesting and fraud.	1	
7	**DATA LEAKAGE PREVENTION :** API responses requests should be inspected to detect sensitive data (CCN/SSN/ID etc.) and mask it.	1	
8	**API QUOTA MANAGEMENT :** API protection solution should limit the number of API calls during a configurable timeframe per API endpoint and per source.	1	
9	**Cloud Managed Security services (API) :** a) Fully-managed onboarding process for new applications and Users b) Ongoing review and optimization of security policies – eliminating false positives c) Real-time support by OEM's Emergency Response Team	1	
	Unified Management - Self-Service Portal Technical Specifications :	**2**	
1	Cloud WAF should provide a real-time single management console to manage multiple Cloud WAF instances protecting multiple websites. The dashboard should contain data such as top attacks view, traffic monitoring view etc.		
2	Should have Unified Portal for Cloud WAF, API Protection, BOT Protection, Integrated DDoS service.		
3	Cloud Cloud WAF should provide Application Analytics		
	a. Cloud Cloud WAF Application Analytics must consolidates large number of similar events into manageable sets of recurring activities to effectively handle		
	b. Security events provided should have context on application behaviour and why certain events are blocked or allowed, displaying key activity details such as recurrence and usage trends over time		
	c. Cloud Cloud WAF Portal should provide drill-down about security events and patterns, including context & clarify into application behaviour like Attack details, HTTP request, Vulnerabilities, origin country of attacker, OWASP Category of attack event falls into and many more		

4	Proposed Solution should be able to create sub accounts and each sub account should have following functionality -Each sub account should have ability to reserve its own bandwidth limit, validity period and No.of application -Each sub account should have visibility or utilization of allocated bandwidth and application -Each sub account should have capability to be categories as demo, POC & production -Each Sub account should role based access to limit visibility to its own sub account		
	OEM Fully Managed Services :	**2**	
1	**OEM must provide** - 24x7 support (portal/email/phone), - 30 minute response SLA via phone, - Onboarding assistance, - Asset health monitoring, - Proactive automatic security anomaly alerts, - On-demand policy tuning, - Configuration management and application security insights - Provision for Post-attack forensics and recommendations		
2	There should be continuous asset-health monitoring for on-boarded application		
3	There should be support & assistance available for False Positive/False Negative correction		
4	There should be Proactive automatic security-anomaly alerts		
5	There should be provision for Post-attack forensics and recommendations		
6	There should be Periodic security-status reporting		
7	There should be mechanism to enable Priority service-case handling.		
8	Should have 24x7x365days Cloud attack detection and alerts capability		
9	The services should be comprehensive and managed services from OEM and includes but not limited to Configuration, Operations, monitoring, fine-tuning of policies, Management etc.		
	Cloud PoP Level Quality & Security Certifications		
1	ISO 27001:2022 (Information Security Management Systems)	2	
2	ISO 27032:2023 (Security Techniques -- Guidelines for Cybersecurity)	2	
3	ISO 27017:2015 (Information Security for Cloud Services)	2	
4	ISO 27018:2019 (Information Security Protection of Personally identifiable information (PII) in public clouds)	2	
5	ISO 27701:2019 (Privacy Information Management System)	2	
6	ISO 28000:2022 (Specification for Security Management Systems for the Supply Chain)	2	
7	PCI-DSS (Payment Card Industry Data Security Standard)	1	
8	US SSAE16 SOC-2 Type II	2	

9	US SSAE16 SOC-1Type II		
10	Should be NSS Lab Certified		
11	Should be ICSA Lab Certified		
12	Should have at least 50+ PoPs globally and PoP level redundancy should be available.	1	

URL Details are as follows

Application Type(WEB / API)	Total URL	Total Domain
WEB	11	4

Technical Evaluation (Stage 2)

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

Stage 3: Financial Evaluation

Financial Evaluation will be carried out only for vendors who qualify through Stage 2.

The financial proposal will be evaluated to identify the most cost-effective and value-driven solution.

(1) Validity of bid:

Bid should be valid for a minimum period of **90 days** in the event of delay in issuance of Purchase Order (PO) by SSL.

(2) Delivery of Service :

Bidder / Vendor should complete the work within 30 days from the date of purchase order(s)

(3) System and System for Tools:

Vendor will make the arrangement of systems for installation of Tools along with software license etc for Load Testing of applications.

(4) Payment Terms:

Sr. No.	Description	Total Amount in %age
1	After Acceptance of PO, Implementation of WAF For All URLs submission of 05% Bank Guarantee, signing of SLA and NDA (01st Quarter)	25%
2	Remaining 75% amount on every Quarter ended (02nd , 03rd and 04th Quarter)	25%

- Applicable Tax Extra

Taxes & levies:

Applicable taxes at actual as per prevailing rate of taxes as per Government notification. Applicable deduction if any may / will be recovered (deducted) from the payment(s)

Stage 4: Selection of Vendor

Stage 2 – Evaluation of Technical Bid

All technical bids of bidders who have qualified Stage A will be evaluated in this stage and a technical score would be arrived at. SSL will scrutinize the offers to determine their completeness, errors, omissions in the technical and commercial offers of respective bidders. SSL may, at its sole discretion, waive any minor non-conformity or any minor deficiency in an offer. SSL reserves the right for such waivers and the SSL's decision in the matter will be final.

Bidders scoring at least 70 marks or more will be declared technically qualified.

Attested photocopies of all relevant documents / certificates should be submitted as proof in support of the claims made. The bidder should provide relevant additional information wherever required in the eligibility criteria. The SSL reserves the right to verify /evaluate the claims made by the bidder independently. 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 SSL. Any decision of SSL in this regard shall be final, conclusive and binding upon the bidder.

Those bidders who meet the threshold score of 70 or more will be considered as "Qualified under Stage 2" and will be considered for evaluation under Stage 3.

Those who do not meet the above threshold will not be considered for further evaluation.

Technical Evaluation

The Technical score Tx = Score from Eligibility Evaluation.
The Relative Technical Score (RTS) for the Bidders will be calculated based on the following basis:

RTSx = (Tx/ T1) *100

Where,
RTSx: Relative Technical Score of each Bidder
Tx : Technical Score of the Bidder
T1 : Technical Score of the Bidder with Highest Tx
Up to 4 decimal values will be considered for the score.

Commercial Evaluation

The Bids which are qualified in Technical would be considered for Commercial Bid evaluation. The vendor should furnish their price for the project in their Commercial Bid to facilitate the commercial evaluation process.

Computation Methodology for Commercial Score

- 70% weightage will be assigned to the Relative Technical Score (RTS) and 30% weightage will be assigned to the Relative commercial score (RCS).
- The Relative Commercial Score (RCS) for each shortlisted Consultant will be calculated as given below:

RCS = L1 / L * 100

Where,
RCS: Relative Commercial Score L:
Amount quoted by the bidder
L1: Lowest Amount quoted by lowest quoted (L1) proposal

Final Evaluation

The final selection of a Bidder will be based on the outcome of the combined Technical & Commercial Evaluation process for the qualified bidders in the Technical Bid round.

The Final Evaluation of Score (FES) will be as below:

FES = 0.70 * RTSX + 0.30 * RCSX

Where:
FESX = Final Evaluation Score of Vendor X
RTSX = Relative Technical Score of Vendor X
RCSX = Relative Commercial Score of Vendor XT

The contract will be awarded to the bidder having the highest Final Evaluation Score (FES) which is an outcome of Techno-Commercial Evaluation process. In case of a tie in the combined score between bidders, the bidder with higher technical score will be given a higher rank.

In the eventuality that less than two eligible bids are received against this RFP, StockHolding reserves the right to proceed with the single bidder or cancel the RFP at its sole discretion.

Clarifications regarding RFP Document, Bid Preparation & Submission of Bid

E-RFP Process

This RFP will follow e-tendering process (e-Bids) which will be conducted by SSL's authorized e-tendering GeM e-Portal.

Performance Bank Guarantee

- Successful Bidder has to submit 10% of total PO value as a Performance Bank Guarantee signing of contract as per timelines defined in the RFP.
- The Performance Bank Guarantee will be released after 3 months of completion of project.

Force Majeure:

Neither the SSL nor the Bidder shall be responsible for any failure to fulfill any term or condition of the CONTRACT if and to the extent that fulfillment 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 defense 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 testing duration exceeds thirty (30) days then, SSL 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 SSL, shall be final and binding on the bidder.

Dispute Resolution:

In the event of any dispute arising out of or in connection with this purchase order, the parties shall use their best endeavor 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) SSL reserves the right to alter the RFP terms and conditions at any time before submission of the bids.

(b) SSL reserves the right to cancel the RFP/contract.

(c) SSL reserves the right to purchase similar service from anyone else within contractual period should the need arise at same rate.

(d) SSL reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. SSL's decision in this regard will be final and binding on all bidders.

No Commitment to accept lowest or any other bid (RFP):

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

Integrity Pact:

The bidder will have to enter into an Integrity Pact with STOCKHOLDING Services Limited. The format (text) for the Integrity Pact is provided as **Annexure - 7**. The bidder will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory.

Non-Disclosure Agreement (NDA):

The successful bidder will sign a Non-Disclosure Agreement (NDA) with Stockholding Services Limited.

Indemnify

The bidder should hereby indemnify, protect and save *SSL* 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 *SSL* is used should be done only with the explicit permission of *SSL*.

Exit clause

SSL reserves the right to terminate this Agreement by giving 1 month notice, if it is not satisfied with the Services. Reasonable number of incidents of the non-performance of the obligations by the bidder as per this Agreement will be provided before the termination notice is served on the bidder. In case of termination, payments due till the date of termination only would be paid based on satisfactory report submitted by bidder and SSL

acceptance. Balance payment for remaining Agreement Term will not be paid to the bidder.

Order Cancellation

SSL reserves the right to cancel the order in the event of the Bidder failing to deliver services as specified by SSL as per the Service Level Agreements. SSL reserves full right and authority to cancel such order and will also be entitled to claim liquidated damages for the same in addition to and without prejudice to all other rights and remedies that may be available to SSL. In case of serious discrepancy in services provided, SSL may cancel the entire purchase order.

Sub-Contracting

No Sub-Contracting is allowed for this RFP.

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.

Sr. No.	Parameters	Response	
1	Name of the Firm/Company		
2	Year of Incorporation in India		
3	Names of the Partners/Directors		
4	Company PAN no		
5	Company GSTN no. (please mention for all		
4	Name and Address of the Principal Banker		
5	Addresses of Firm/Company		
	a) Head Office		
	b) Local Office in Mumbai(if any)		
6	Authorized Contact person		
	a) Name and Designation		
	b) Telephone number		
	c) E-mail ID.		
7	**Financial parameters**		
	Business Results (last three years)	Annual Turnover (Rs. in Crores)	Operating Profit (Rs. in Crores)
	2022-23		
	2023-24		
	2024-25		
	(Only Company figures need to be mentioned not to include group/subsidiary Company figures}	(Mention the above Amount in INR only)	
	Details of Reference Customer		
	Customer Name and Contact No.	Brief Details of hardware supplied	PO number and Date(Attached PO with masked price)
	1		
	2		
	3		
	4		

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

Dated this..... Day of 2026

(Signature)

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

Note:

1. Letter of Authorization shall be issued by either Managing Director having related Power of Attorney issued in his favour or a Director of the Board for submission of Response to RFP/ Tender.
2. All self-certificates shall be duly signed and Stamped by Authorized signatory of the bidder Firm unless specified otherwise.
3. Bidder response should be complete; Yes/No answer is not acceptable...
4. Details of clients and relevant contact details are mandatory. Bidder may take necessary approval of the clients in advance before submission of related information. SSL will not make any separate request for submission of such information.

-

Commercial Bid Format

Sr. No	Requirement	Price (Rs.)	Remark
1	WAF System for 4 Domains having 11 URL including services mentioned as per Technical Criteria		PDF File need to be submitted with next 2 years quote
2	Additional URL		Yearly Price and next 2 years quote

Note: Above prices should be inclusive of taxes & levies

Commercial Bid

a. The vendor / bidder will submit Commercial Bid online on GEM portal mentioned above as per format provided.
b. The final price (L1) will be decided only on successful evaluation.

Dated this..... Day of 2026

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

RFP For WAF For SSL Setup

Annexure - 6 - Covering Letter-1

(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, *SSL* ., a company incorporated under Companies Act, 1956, with its Registered Office Plot No. P-51, T.T.C. Industrial Area, MIDC, Mahape, Navi Mumbai - 400 710 acting through its authorized officer, (hereinafter called **Principal**), which expression shall mean and include unless the context otherwise requires, his successors in office and assigns) of the First Part **And** M/s._____ _____(with complete address and contact details) represented by Shri_____(i.e. s (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 endeavour 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 / *SSL* 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, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PRINCIPAL, connected directly or indirectly with the bidding process, or to any person organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.
3. The Counter Party further undertakes that it has not given, offered or promised to give directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Principal / *SSL* 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 / *SSL* for forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the

Principal / *SSL*.

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 / *SSL* 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 / *SSL* 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 Technical Bid, as given at Annexure 6. If bids are invited through a Consultant a Declaration has to be submitted along with the Technical Bids as given at Annexure.
8. The 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 *SSL* /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 / *SSL* as part of the business relationship, regarding plans, technical 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 / *SSL*, or alternatively, if any relative of an official / employee of Principal / *SSL* 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 / *SSL*
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 / *SSL* 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 / *SSL*. Such exclusion may be for a period of 1 year to 3 years as per the procedure prescribed in guidelines of the Principal / *SSL*.
2. The Bidder / Contractor / Counter Party accepts and undertake to respect and uphold the Principal / *SSL'*s absolute right to resort to and impose such exclusion.
3. Apart from the above, the Principal / *SSL* may take action for banning of business dealings / holiday listing of the Bidder / Counter Party / Contractor as deemed fit by the Principal / Owner / *SSL*.
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/ *SSL* 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 / *SSL* / Owner under Law or the Contract or its established policies and laid down procedure, the Principal / *SSL* / 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 / *SSL* / 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 / *SSL* / Owner apart from exercising any legal rights that may have accrued to the Principal / *SSL* / 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 / *SSL* 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 / *SSL* has substantive suspicion in this regard, the Principal / *SSL* / Owner will inform the same to the Chief Vigilance Officer through the Vigilance Officer.

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

1. The Principal / *SSL* / Owner will enter into Pacts on identical terms as this one with all Bidders / Counterparties and Contractors.
2. The Principal / *SSL* / Owner will disqualify Bidders / Counter Parties / Contractors who do not submit, the duly signed Pact, between the Principal / Owner / *SSL* 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 / *SSL* has appointed competent and credible Independent External Monitor (s) (IEM) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Integrity Pact.
2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Chief Executive Officer and Managing Director, Stock Holding Corporation of India Limited.
3. The 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 / *SSL* / 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 Tender (RFP) Documentation / papers / files. The IEM is under contractual obligation to treat the information and documents of the Bidder(s) / Contractor(s) / Counter Party (ies) with confidentiality.
4. In case of tender (RFP)s having value of 5 crore or more, the Principal / *SSL* / 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 /*SSL* and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit non-binding recommendations. Beyond this, the IEM has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The IEM will submit a written report to the CEO&MD, *SSL*. Within 6 to 8 weeks from the date of reference or intimation to him by the Principal / Owner / *SSL* and should the occasion arise, submit proposals for correcting problematic situations.
7. If the IEM has reported to the CEO&MD, *SSL* Ltd. a substantiated suspicion of an offence under the

relevant IPC/PC Act, and the CEO & MD, *SSL* 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 *SSL*

VIII. VIII. Other Provisions

1. This IP is subject to Indian Law, place of performance and jurisdiction is the Head Office / Regional Offices of the SSL /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 / *SSL* 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 / *SSL*

(For and on behalf of Bidder / Counter Party / Contractor)

WITNESSES: 1._____

2._____

(Signature, name and address) (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.

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

Date:

To,

Sub**:** RFP No: **_____ dated _____ for REQUEST FOR Procurement of WAF System**

Dear
Sir,

DECLARATION

Stock Holding Corporation of India Limited (*SSL*) hereby declares that *SSL* 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 tenderer / bidder will stand disqualified from the tendering 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 the *SSL*

Yours faithfully,

For and on behalf of Bidder
(Authorized Signatory)

RFP For Procurement of WAF System

Annexure - 8 - Compliance Statement

(To be submitted along with technical bid)

Subject: **RFP For Procurement of WAF System**

Ref: RFP **No: _____ dated _____**

DECLARATION

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

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

Dated this..... Day of 2026

(Signature)

(In the capacity of)

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

RFP For Procurement of WAF System

(To be submitted along with Technical Bid)

To,
STOCKHOLDING Services Ltd.
STOCKHOLDING House, Plot No. P-51, T.T.C. Industrial
Area, M.I.D.C., Mahape, Kalyan-Shil Road,
Navi Mumbai, PIN 400710.

Dear Sir,

Sub**:** RFP No: _____ dated _____ **RFP For Procurement of WAF System**

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

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

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

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

SSL is not bound to accept the lowest or any bid received by *SSL*, and it may reject all or any bid. If our bid is accepted, we are responsible for the due performance of the contract.
Dated this..... Day of 2026

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