Stock Holding Corporation of India Limited

(StockHolding)

RFI Reference Number

RFI/IT/01/2024-25 Date:24th Feb2025

Request for Information (RFI) For Conducting Proof of Concept (PoC) for procurement & implementation of On Premise Next Gen Perimeter Firewall (NGFW)

DISCLAIMER

This **Request for Information (RFI)** is NOT a Request for Proposal, Invitation for Bid, or announcement of a solicitation. It is intended for information or planning purposes only. There is no bid package or solicitation document associated with this announcement. Response to this RFI is strictly voluntary and will not affect any potential participant's ability to submit an offer if a solicitation is released. Any requests for a solicitation package will be disregarded. The Corporation does not intend to award a contract on the basis of this RFI or otherwise pay for the information solicited. No entitlement to payment of direct or indirect costs or charges by the Corporation will arise as a result of preparing submissions in response to this RFI and the Corporation use of such information. Respondents of this RFI may be requested to provide additional information/details based on their initial submittals.

This Request for Information (RFI) is being floated by the Stockholding on behalf of Information Technology Department, for the purpose of identifying organizations who are willing to participate in "**Conducting POC for On-premise Next Gen Perimeter Firewall**" with robust, implementable, innovative, cost effective and scalable technology options.

1. Background

StockHolding Corporation of India Limited (StockHolding) would like to request information from experienced and reputable Original Equipment Manufacturers (OEM's) specializing in "**On-premise Next Gen Perimeter Firewalls**" solutions for conducting a Proof of Concept (POC) for procurement & implementation of Next Gen Perimeter Firewalls (NGFW).

2. Objective

The primary objective of this Request for Information (RFI) is to gain a better understanding of the On-Premise Next Gen Perimeter Firewalls for Data Centre (DC) and Disaster Recovery Centre (DR) available in the market and the associated cost models. To keep pace with technological advances, it is necessary to periodically evaluate existing Firewall solutions through detailed Proof of Concept (PoC) of new solution available in the market.

PoC Period

PoC need to be completed with-in 30-45 days by each OEM after declaration of shortlisted vendors. Schedule will be informed to the OEM's accordingly.

Scope of Work (SOW)

We are interested in receiving proposals "**On-premise Next Gen Perimeter Firewalls**" Solution supporting the following key functionalities:

- Product should have capability to create virtual Tenants
- Should be able to support security features like IPS, DDOS etc.
- Should have VPN capability
- The proposed system should have integrated Traffic Shaping functionality
- The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Should also support enablement of Vmware NSX and Oracle NSG
- The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types (http, https, smtp etc.) and per firewall policy
- The proposed system shall provide web content filtering features
- Should be able to work in High availability and support stateful session

Features to be Demonstrated during PoC is attached in **Annexure – III**

3. Shortlisting Criteria

Below is the list of Eligibility criteria that would be followed to short list bidders.

Sr. No.	Criteria	Documents to be provided
1	The Bidder should be a company registered under the Indian Companies Act, 2013 and operational for the last five years.	Certificate of incorporation
2	The OEM's should have a minimum average turnover of Rs. 100 Crores for the last 3 audited Financial Years (2021-22, 2022-23, 2023-24) with profit in the last three financial years	Copy of the audit Annual Reports and /or certificate of the Chartered Accountant
3	Minimum 03 (three) references where bidder has implemented similar projects for last 3 years in BFSI	Self-declaration with address and contact details on company's letter head signed by the company's authorized signatory
4	Vendor to have registered office in Mumbai / Navi-Mumbai / Thane for providing service	Relevant document confirming the same is required
5	The proposed solution should be listed in Gartner's Top Quadrant	Latest Gartner Quadrant Snapshot

4. Solution Requirements

Interested vendors/service providers are requested to submit the following:

1. A detailed pre-requisite document for StockHolding to setup the required infrastructure.
2. The proposal should contain details of the appliances that will be used in conducting the POC.
3. Contact details of Single Point of Contact from the OEM Side (SPOC)
4. Budgetary estimates post conclusion of the POC and based on StockHolding's requirements.

5. Procedure for Submission of RFI

All interested, capable and responsible sources that wish to respond to this RFI are required to email their responses (.doc or .pdf format) to **ITPROC@stockholding.com** not later than 18:00 HRS IST**, 31st Mar 2025**. "**POC for on premise Next Generation Perimeter Firewall**" must be included in the subject line. Telephonic responses will not be accepted.

Last date for submission of documents : 15th Mar 2025.

Expected start of POC at StockHolding Premises: 15th Apr 2025.

Site Address for POC:
Stockholding Corporation of India Limited,
Plot No. P-51, TTC Industrial Area, MIDC, Mahape, Navi Mumbai – 400710
Maharashtra, India

Any information required for OEM's from StockHolding shall be provided during the POC stage.

We look forward to receiving your submission and potentially collaborating with your team to implement the Next Gen Perimeter Firewall solution and enhance security. Should you have any questions or require further clarification, please do not hesitate to reach out to us at **ITPROC@stockholding.com**

6. Instruction to Bidders

6.1 Language of RFI Preparation

The RFI response prepared by the RFI Participants and all correspondence and documents relating to the RFI responses exchanged by the RFI Participants and StockHolding, shall be written in the **English** language.

6.2 Clarification

If deemed necessary, StockHolding may seek clarifications on any aspect from the participants. However, that would not entitle the RFI Participants to change or cause any change in the substance of the response submitted.

6.3 Right to Accept/Reject any or all RFI Responses

StockHolding reserves the right to accept or reject any RFI and to annul the tender process and reject all RFI responses at any time prior to award of the contract, without thereby incurring any liability to the affected RFI Participants or any obligation to inform the affected RFI Participants of the grounds for StockHolding's action.

StockHolding reserves the right to accept or reject any/all RFI solution if the solutions are not up to the mark.

6.4 General Instructions –

- StockHolding shall not pay for any information or administrative costs incurred in response to this RFI. All costs associated with responding to this RFI will be solely at the participant's expense.
- This RFI is a separate and independent process and is issued solely for information and planning purposes. It does not constitute a Request for Proposal (RFP) or a promise to issue a RFP in the future.
- This RFI does not commit the StockHolding to contract for any supply or service whatsoever. StockHolding is not currently seeking proposals and will not accept unsolicited proposals.
- The response to this RFI will not be used to pre-qualify vendors.

Annexure – I

(Eligibility Criteria)

Implementation of StockHolding Next Gen Perimeter Firewall:

Sr. No.	Criteria	Documents to be provided
1	The Bidder should be a company registered under the Indian Companies Act, 2013 and operational for the last five years.	Certificate of incorporation
2	The OEM's should have a minimum average turnover of Rs. 100 Crores for the last 3 audited Financial Years (2021-22, 2022-23, 2023-24) with profit in the last three financial years	Copy of the audit Annual Reports and /or certificate of the Chartered Accountant
3	Minimum 03 (three) references where bidder has implemented similar projects for last 3 years	Self-declaration with address and contact details on company's letter head signed by the company's authorized signatory
4	Vendor to have registered office in Mumbai / Navi-Mumbai / Thane for providing service	Relevant document confirming the same is required
5	The proposed solution should be listed in Gartner's Top Quadrant	

Authorized Signatory:

Name of the Authorized

Signatory: Place:

Date:

Seal:

Annexure-II

(RFI Submission FORM)

(To be submitted on the letterhead of the Company)

Date: _____

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

Dear Sir,

Subject: Submission of the RFI – "Implementation of On-premise Next Generation Perimeter Firewall"

We, the undersigned, offer to provide services for Implementation of On-premise Next Generation Perimeter Firewall its operational management System to StockHolding in accordance with your Request for Information (RFI) – Implementation **of On premise Next Generation Perimeter Firewall** dated **24th Feb 2025**. We are hereby submitting RFI.

We hereby declare that all the information and statements made in this RFI are true and accept that any misinterpretation contained in it may lead to our disqualification.

We agree to abide by all the terms and conditions of the RFI document. We understand that you are not bound to accept any proposal you receive.

Yours sincerely,

Authorized Signature [In full and initials]: _____

Name and Title of Signatory: _____

Name of Firm: _____

Address: _____

Location: _____Date: _____

Annexure – III
(Features/ Requirements to be Demonstrated during POC)

Sr No	Specifications	POC Requirement Comments
	1. Hardware	
1.1	Firewall appliance should have Console port and USB Ports.	
1.2	Appliance should be rack mountable and included with support side rails if required.	
1.3	Firewall should have Hardware Sensor Monitoring capabilities.	
1.4	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Firewall appliance architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc). Control plane must have dedicated resources such as CPU, RAM etc. This is to ensure Stockholding Corporation always has management access to NGFW irrespective of Firewall load / Traffic Spike / Cyber Attack driving higher CPU utilization. Stockholding Corporation should able to login to the firewall and carry out reporting / management / packet capture etc. to identify the root cause and accordingly take necessary action to remediate it.	
1.5	The platform should support VLAN tagging (IEEE 802.1q)	
1.6	The firewall should support ISP link load balancing. Stockholding should able to terminate links on firewall appliances.	
1.7	Firewall should support Link Aggregation functionality to group multiple ports as single port.	
1.8	Firewall should support Ethernet Bonding functionality for Full Mesh deployment architecture.	
1.9	The proposed system should be able to operate in Transparent (Access) mode and NAT/Route mode.	
1.10	The physical interface should be capable of link aggregation as per IEEE 802.3ad standard, allowing the grouping of interfaces into a larger bandwidth 'trunk'. It should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk	
	2. Performance Requirement	

2.1	Setup-1: The proposed firewall must provide minimum 14 Gbps of NGFW throughput with Application control and logging enabled, utilizing AppMix transactions	Via Simulation if possible
2.2	Setup-2: The proposed firewall must provide minimum 9 Gbps of NGFW throughput with Application control and logging enabled, utilizing AppMix transactions	Via Simulation if possible
2.3	The Firewall Appliance shall be capable of Application Control, IPS, antivirus, antispyware, Anti-malware, DNS Security, file blocking, IDS & IPSc, Anti-Spywared, Anti-Botnete, Anti-APT, Logging and Reporting, Application Identification, Firewall.	Via Simulation if possible
2.4	The proposed appliance must support minimum 1.4 Million concurrent sessions with Real world HTTP applications and not based on UDP / Lab environment / ideal testing environment.	Via Simulation if possible
2.5	The proposed firewall must support minimum 140,000 new session per second.	Via Simulation if possible
2.6	The Proposed NGFW should have a capability to support minimum 600 Remote VPN users supporting Windows , MAC , Linux endpoint Operating Systems	Via Simulation if possible
2.7	The proposed NGFW should be capable to create 4 virtual instances within the firewall instead of multiple firewalls to separate the segments and the subscriptions to be included from day 1	Create at least 2 instances
	3. NGFW Features	
3.1	It must allow to create security policies based on L7 parameters such as Application, Users, File Type etc in addition to IP & Port numbers.	
3.2	While creating application-based policy the firewall must auto select all default port numbers without need of admin to mention it separately. Example - while allowing Active Directory as an application, firewall must auto include all relevant port numbers used for AD communications such as 135, 138, 139, 389, 445 etc.	
3.3	While creating application-based policy the firewall must inform admin about dependent application to be included in the policy to avoid application misbehaviour. Example Active Directory application is dependent on "kerberos, ms-ds-smb-base, ms-netlogon, netbios-dg, netbios-ns, netbios-ss" applications. While Allowing Active Directory communications, NGFW must alert security admin to include these applications in the policy as well.	
3.4	The firewall must able to identify users behind Proxy server by reading information in XFF header and perform User mapping. The firewall must strip XFF information before forwarding traffic to internet for privacy reason.	
3.5	The Firewall must support Active - Passive & Active - Active deployment option with seamless failover between HA pairs.	

3.6	The proposed firewall must support dynamic security policy to self-adjust & updated based on received IOC without needing to commit the Firewall Configuration. Example - Stockholding Corporation can configure NGFW to ingest threat feed from a central Server within Stockholding Corporation. Once this information is added in to this central server, all NGFW must ingest this IOC in an automated fashion and update security policy instantly. The policy update should be completed within 10 minutes & new IOC should be should be added in Firewall Config & firewall should start blocking traffic.	
3.7	The firewall must able to identify end user ip addresses even if user traffic is coming via content delivery network example Akamai by reading information in XFF header. The Firewall must allow Stockholding Corporation to create security policy based on IP Address information in XFF. Example - If Stockholding Corporation want to block bad ip addresses from China, Firewall must able to detect these Bad IP Addresses even if Chinese attackers are coming via Akamai CDN in USA / Europe / India and hiding their original source IP with Akamai IP. NGFW as source IP and block such traffic instantly.	
3.8	The NGFW must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count limit for the capture.	
3.90	The firewall must support FQDN instead of IP address for static route next hop, policy based forwarding next hop and BGP peer address	
3.10	The proposed solution must support Policy Based forwarding based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports	
3.11	The proposed solution should support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application (such as Skype, BitTorrent, YouTube, azureus) -by static or dynamic application groups (such as Instant Messaging or P2P groups) -by port and services	

3.12	The NGFW must provide immediate visibility into Covert communication traversing in Stockholding Corporation environment without any manual effort and additional configurations required. This should be Plug-n-Play feature. Applications bypassing traditional security policy & running on nonstandard ports in the Stockholding Corporation environment. The Firewall must able to provide comprehensive report with Source/Destination IP, Application name (real application name & not protocol), source & destination Zone, data transfer amount & file name transfer. So Stockholding Corporation team can take preventive action accordingly. Example DNS application running on any other port then 53.	Via Simulation if possible
3.13	The users should not be able to uninstall or Disable the VPN Agent installed on the users machines unless until mandated by Stockholding Corporation Security Team	
3.14	The Remote Access VPN solution should provide automatic connectivity to VPN immediately after user logs in to his machine so that all the endpoint VPN traffic is routed securely through Stockholding Corporation NGFWs while the users are working remotelyThe Remote Access VPN Solution must also have the capability to connect VPN when the user machines starts/boots-up so as to have Secure VPN tunnel build up even before the user logs in to the machine. This will help Stockholding Corporation to have secure VPN connectivity and visibility across all network traffic going out of the end users machine	
3.15	The VPN solution should have the Ability to block full network access if client is unable to connect to cloud gateway	
3.16	The VPN solution should have the Ability to block full network access and allow only specific IP/host/portals when client is enable to connect to cloud gateway	
3.17	The Remote Access VPN solution should have a User/device Posture Assessment - Certificate check, Domain check, Antivirus / Antimalware agent check, Custom apps check, Patch management check, process and registry check on endpoints so as to make dual inspection with posture + user authentication before user connects to Stockholding Corporation Infrastructure.	
	4. Security Features	
4.1	The firewall must support comprehensive threat prevention security features including IPS, Antivirus, Anti Spyware, Anti Bot, DoS/DDOS, File Blocking etc from day one.	Via Simulation if possible
4.2	The proposed firewall must have integrated Intrusion Prevention Systems - IPS with ability to prevent Stockholding Corporations critical IT/OT applications and digital assets against minimum 19,500 + vulnerability exploit attempts. The firewall must detect & prevent minimum 14,000 + CVE exploit attempts to safeguard Stockholding Corporation environment. OEM to provide full list of IPS signatures along with CVE numbers.	

4.3	The proposed firewall must support attack recognition for IPv6 traffic the same way it does for IPv4	
4.4	The proposed solution must support different actions in the policy such as deny, drop, reset client, reset server, reset both client and server.	
4.5	The proposed solution must have functionality of Geo Protection to Block the traffic country wise per policy and per applications as per customer requirement and shouldn't be a global parameter	
4.6	The proposed solution must have an option to create your own signatures using SNORT. The firewall must provide IPS Signature Converter to automatically convert Snort and Suricata rules into custom threat signatures instead of manually performing the process of creating signature.	
4.7	The Firewall must support ability to decrypt & inspect TLS 1.3 traffic.	
4.8	The proposed firewall must support ingesting 3rd party IOCs such as IP Addresses, Domain Names & URLs from different sources including existing security solution such as FireEye, Crowdstrike & Open source threat intel such as Talos, Spamhouse etc. NGFW must automatically update the Security policy in less than 10 minutes without requiring any manual intervention and commit required by Security Admin. The traffic must be blocked to & from such IOC in less than 10 minutes.	
4.9	The proposed firewall should have the ability to create custom application signatures and categories directly on firewall without the need of any third-party tool or technical support. Also the device should have capability to provide detailed information about dependent applications to securely enable an application	
4.10	All the proposed threat prevention functions like IPS/vulnerability protection, Antivirus, C&C protection etc. should work in isolated air gapped environment without any need to connect with Internet.	
4.11	The NGFW must provide list of applications using TLS1.0, TLS1.1, TLS1.2 & TLS1.3 in Stockholding Corporation environment so that Stockholding Corporation team can disable weaker TLS protocol on given applications. Additionally NGFW must provide list of SSL application using SHA-1 (weaker cipher) so Stockholding Corporation team can work with application team to change SHA-1 with SHA-2.	
4.12	The NGFW must block & sinkhole queries made to malicious domain DNS queries. The NGFW must respond back with a fake IP or Loop Back IP so NGFW must identify the real end user or infected machine trying to connect to malicious domains. Since DNS request traverse through multiple servers it is impossible to identify the real users & infected machine. DNS Sinkholing will help block malicious request and help identify the real user / machine as well. So Stockholding Corporation can reach out to user / machine and remediate it.	Via Simulation if possible

4.13	The NGFW Anti virus & anti Malware must able to analyse & prevent malicious file, virus, malware, ransomware etc. traversing on following protocols: HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP, and SMB.	Via Simulation if possible
4.14	The NGFW must be able to support decryption of the following protocols: SSL, SSH	
4.15	The proposed NGFW must identify over provisioned security rule configured in NGFW using AI / ML technology. The NGFW must provide comprehensive details with list of applications traversing on each security policies over a period of time. NGFW must provide information about number of days since no new app observed, bytes transferred by specific security rule & total number of applications observed on security policy to provide confidence to operation team to fine the security policy. NGFW must offer quick rule optimization to allow only business applications and block unwanted applications. The NGFW must provide report of over permissive rule & unused rule over a period of time such as 30 / 90 days etc.	
4.16	The NGFW must provide seamless approach to migrate existing L3/L4 policies to L7 Application based policies without any disruption. The migration must be completely risk free and automated. The OEM must have a mature migration tool to migrate configuration seamlessly. The migration tool must preserve Comments & Description mentioned in existing Rules while migrating it to new NGFW. The migration tool must able to stimulate Stockholding Corporation environment and test migrated config even before applying it to Firewall and need to test it live. So Stockholding Corporation can minimize the failure risk during migration.	
4.17	Same Hardware platform should be scalable to provide URL filtering and web protection and should maintain same performance/throughputs mention in primary scope	
4.18	The proposed NGFW firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.	
4.19	The solution must employ a cloud sandbox analysis engine using virtual execution to detect zero day and unknown threats and must not be reliant only on signatures.	
4.20	The Sandbox functionality of proposed solution should utilize a state-full attack analysis including Bare-Metal Analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.	
4.21	The Sandboxing environment should provide an update signature in real time or less than equal to 5 minutes for unknown threats. Sandbox can be On-Prem or Cloud Sandbox , If cloud Sandbox is proposed then the Cloud Sandboxing Environment should be available within India	

4.22	The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures	
4.23	The solution should have a provision of URL filtering service and the same should be able to categorize a site by multiple categories and not just a single and custom category	
4.24	Should protect against never-before-seen phishing and JavaScript attacks inline. Solution should be capable to use both signature based and ML based signature less technology	Via Simulation if possible
4.25	The NGFW should prevent this kind of credential theft attack (without the need of endpoint agents). Vendors should provide features with the ability to prevent the theft and abuse of stolen credentials, one of the most common methods cyber adversaries use to successfully compromise and maneuver within an organization to steal valuable assets. It should also complement additional malware and threat prevention and secure application enablement functionality, to extend customer organizations' ability to prevent cyber breaches. 1. Automatically identify and block phishing site 2. Prevent users from submitting credentials to phishing site 3. Prevent the use of stolen credentials	Via Simulation if possible
4.26	The proposed solution must support protection/mitigation against Fast Flux DNS, Ultra-Slow DNS Tunnelling, Dictionary DGA, Dangling DNS, and Malicious Newly Registered Domains types of attacks.	
4.27	Should support prevention against advance DNS based attacks trying to abuse DNS Protocols. proposed solution should support DGA Based attacks, Cybersquatting attacks.	
4.28	The Solution must have DLP controls to allow/block specific file types for upload / download such as PDF, Office, Password protected ZIP? The controls should apply even if user has changed the extension.	
4.29	The Solution must support Machine Learning Pattern based DLP controls to block/alert on transfer of specific patterns such as Aadhar Card, PAN Card, Source code, Legal documents, financial documents.	
4.30	The Solution must support proximity detection for DLP Pattern matching to reduce false positives and increase accuracy of the DLP solution.	
4.31	The Solution must support Data Fingerprinting based DLP to enable organization to upload their own data / document formats for better accuracy of DLP incidents.	
4.32	The Solution must allow administrators to train their own ML model on the organizations document types to increase accuracy of DLP matching.	
4.33	The Solution must support Optical Character Recognition based DLP to protect from image based data leakage.	
4.34	The Solution must support Exact Data Matching based DLP to protect evidence based dataset leakage.	

4.35	The Solution must support Data Dictionaries to support common phrases keywords in industries. Custom Dictionaries should be supported.	
	5. Management	
5.1	The firewall must support on device management using SSH & HTTPS GUI for management, reporting & config changes in case of emergency & non availability of centralized management.	
5.2	The firewall must have CLI, SSH & HTTPS based on device management	
5.3	The firewall must have fully developed on device management allowing all possible configurations to be performed directly on the firewall.	
5.4	The firewall must have comprehensive logging, log analyser, log correlation, search, filter, unified logs available directly on firewall.	
5.5	The management solution must provide Executive Dashboard - Customizable Dashboard to provide quick insight to Applications / Users / Content / Files / Threat / Top Country / Top Rule Usage	
5.6	The proposed management solution must have the capability to support up to multiple devices at zero cost considering current + future requirements	
5.7	The management solution shall provide a single console to manage all the firewalls and provide visibility across the infrastructure	
5.8	The solution shall allow creation of objects and policies at a central place and allow it to be deployed to the managed devices.	
5.9	The solution shall allow detailed revision tracking of policies and have auditing mechanism to track changes.	
5.10	The solution shall allow configuration backup of the managed devices.	
5.11	The solution shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges.	
5.12	In case of wrong config push / human error resulting in the locations firewalls isolation & loosing communication with centralized management, the firewalls must auto restore last known good config and restore communication with Central management console without any manual intervention.	
5.13	The administrator must be able to import the NGFW configuration into the central management platform	
5.14	The administrator must be able to view report on the CPU usage for management activities and CPU usage for other activities.	
5.15	The firewall must have the ability to manage firewall policy even if management server is unavailable	

5.16	The management solution must have the native capability to optimize the security rule base and offer steps to create application based rules.	
5.17	The NGFW must support the ability to create custom reports directly from the Web GUI of the NGFW	
5.18	The NGFW must support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed	

Annexure – IV

Non-Disclosure Agreement (NDA)

This Non-Disclosure Agreement (hereinafter "Agreement") is executed on this _____ day of _____, 2025 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

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

StockHolding and _____ 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 one (1) year from _____ (the Effective Date). Either Party may terminate this Agreement by giving a ten (10) 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.

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.

8. **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.

9. **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**
Name:	Name:
Title:	Title: