Corrigendum-1 for RFP				
RFP Ref. No.		**CPCM-19/2025-26 (GEM Reference No. - GEM/2025/B/6849585)**		
RFP Name		**RFP for Procurement of Next Generation Firewall**		
Sr. No.	**Pg. No**	**Description**	**Existing Clause**	***Amended Clause***
1	43	Annexure 10 - Technical Specifications 2. Performance Requirement	2.1 Setup-1 (SHCIL): The proposed firewall must provide minimum throughput (mentioned in Table 1.1) of NGFW throughput with Application control and logging enabled, utilizing appmix transactions	*2.1 Setup-1 (SHCIL): The proposed firewall must provide the minimum NGFW throughput (as mentioned in Table 1.1) with application control and logging enabled, utilizing standard IMIX traffic patterns*
2	44	Annexure 10 - Technical Specifications 3. NGFW Features	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	*Mentioned clause is removed*
3	44	Annexure 10 - Technical Specifications 3. NGFW Features	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.	*3.4 The firewall must be able to identify users located behind a proxy server by reading the client IP address from the X-Forwarded-For (XFF) HTTP header for accurate user mapping. The firewall must support removing or anonymizing XFF information before forwarding traffic to external networks to maintain user privacy.*
4	45	Annexure 10 - Technical Specifications 3. NGFW Features	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	*3.11 The proposed solution should support the ability to create QoS policy on a per rule basis:* *-by source address* *-by destination address* *-By Port and services*

Sr. No.	Pg. No	Description	Existing Clause	*Amended Clause*
5	46	Annexure 10 - Technical Specifications 3. NGFW Features	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	*Mentioned clause is removed*
6	47	Annexure 10 - Technical Specifications 3. NGFW Features	3.15 The VPN solution should have the Ability to block full network access if client is unable to connect to cloud gateway	*Mentioned clause is removed*
7	47	Annexure 10 - Technical Specifications 3. NGFW Features	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	*Mentioned clause is removed*
8	47	Annexure 10 - Technical Specifications 4. Security Features	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.	*4.6 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 rules into custom threat signatures instead of manually performing the process of creating signature.*
9	49	Annexure 10 - Technical Specifications 4. Security Features	4.32 The Solution must allow administrators to train their own ML model on the organizations document types to increase accuracy of DLP matching.	*4.32 The solution must support accurate DLP detection and allow administrators to create custom rules, patterns, or fingerprints for organization-specific document types to enhance detection accuracy.*
10	51	Annexure 10 - Technical Specifications 5. Management	5.20 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	*Mentioned clause is removed*
Note: All other clauses/Terms & conditions except above shall remain same as per RFP (RFP Reference Number: CPCM-19/2025-26)				