राष्ट्रीय अवसंरचना वित्तपोषण और विकास बैंक (नैबफिड)

National Bank for Financing Infrastructure and Development (NaBFID)

Corrigendum to Supply, installation & maintenance of Cloud Based Secure Web Gateway/ Proxy, Virtual Private Network (VPN)/ Zero Trust Network Access (ZTNA) & Data Loss Prevention (DLP) Solution (Ref: NaBFID / IS / RFP /06 dated July 21,2025)- **GEM Bid Ref No: GEM/2025/B/6477353**

Date of release of the corrigendum: August 05, 2025

Sr No	RFP Clause	Existing Clause	Amended Clause
1.	6 Scope of Work General Requirements	The proposed solution must have in-built data log retention of at least 1 year from for all components.	The proposed solution must have in-built data log retention of at least 1 year from day 1 for all components.
2.	6.1 Cloud Based Secure Web Gateway/ Proxy	The solution shall include Web Proxy with Caching, Web Content Filtering, URL filtering, Anti Malware, Anti-Virus, Application layer filtering, Sanboxing, Layer-7, Application control features etc.	The solution shall include Web Proxy with Web Content Filtering, URL filtering, Anti Malware, Anti-Virus, Application layer filtering, Sanboxing, Layer-7, Application control features etc.
3.	Functional & Technical Requirements: Cloud Based Secure Web Gateway/ Proxy (Sr No .1)	The solution must have a complete license for Web content filtering, Anti-Malware, SSL/TLS Inspection, Content Inspection, Advanced Threat Protection, Application Visibility and Control, Bandwidth Control, Visibility and Control of all ports and protocols, and Advanced Reporting with at least 1-year built in log retention.	The solution must have a complete license for Web content filtering, Anti-Malware, SSL/TLS Inspection, Content Inspection, Advanced Threat Protection, Application Visibility and Control, File size and type-based restriction control during upload and download, Visibility and Control of all ports and protocols, and Advanced Reporting with at least 1-year built in log retention.
4.	Functional & Technical Requirements: Cloud Based Secure Web Gateway/ Proxy (Sr No .3)	The proposed solution must support policy creation based on defined criteria such as users, user groups, device trust status, geographic location, URL categories, cloud applications, destination IP addresses, custom URLs, and similar attributes.	The proposed solution must support policy creation based on defined criteria such as users, user groups, device trust status, geographic location, URL categories, cloud applications, destination IP addresses, custom URLs, and similar attributes. There should not be any limitation in the number of policies that can be created
5.	Functional & Technical Requirements	The solution must have the ability to create custom categories based on URLs	The proposed solution must support the creation and management of custom URL categories and allow

	Cloud Based Secure Web Gateway/ Proxy (Sr No .6)		sufficient scalability, without imposing limitations that could hinder the Bank’s requirements at any point during the project tenure.
6.	Functional & Technical Requirements Cloud Based Secure Web Gateway/ Proxy (Sr No .11)	The proposed solution should have the capability to create custom file-type control policies based on users, groups, type of applications, action type (upload and download) etc.	The proposed solution should have the capability to create custom file-type control policies based on users, groups, type of applications, action type (upload and download) etc. and there should not be any limitation in the number of file types supported by the platform for enforcing necessary control as per Bank's requirement.
7.	Functional & Technical Requirements Cloud Based Secure Web Gateway/ Proxy (Sr No .13)	The proposed solution should have a dynamic risk scoring mechanism to evaluate the potential risk of the URLs accessed by the end users. It should support the auto-blocking of such high risk categorized URLs.	The proposed solution should have a dynamic risk scoring mechanism to evaluate the potential risk of the URLs accessed by the end users. It should support the auto-blocking of such high risk categorized URLs based on the Bank's requirements.
8.	Functional & Technical Requirements Cloud Based Secure Web Gateway/ Proxy (Sr No .18)	The solution should have an inbuilt DNS security solution to ensure safe browsing for end user.	The solution should have an inbuilt DNS security solution which will be robust to DNS attacks like DNS spoofing, DNS tunnelling, DNS amplification attacks etc. to ensure safe browsing through the cloud based secure web gateway.
9.	Functional & Technical Requirements Cloud Based Secure Web Gateway/ Proxy (Sr No .27)	The proposed solution must have the option to schedule automated backups within the admin console to create backups periodically without manual intervention to ensure compliance with the organization's Business Continuity Plans and Disaster Recovery Plans.	The proposed solution must have the option to schedule automated backups within the admin console / with the help of OEM backend support to create backups periodically to ensure compliance with the organization's Business Continuity Plans and Disaster Recovery Plans.
10.	Functional & Technical Requirements Cloud Access Security Broker (CASB) (Sr No .32)	The solution must support the creation of detailed access control policies for Microsoft 365 applications (e.g., OneDrive, SharePoint, Teams), Google applications (e.g., Google Drive, Gmail, Google Doc) etc. including controls over file uploads, downloads, sharing, and security inspection.	The solution must support the creation of detailed access control policies for the complete inspection of Microsoft 365 applications (e.g., OneDrive, SharePoint, Teams), Google applications (e.g., Google Drive, Gmail, Google Doc) etc. as part of data and threat protection scanning along with controls over file uploads, downloads, sharing, and security inspection.

11.	Functional & Technical Requirements VPN/ Zero Trust Network Access (Sr No. 42)	The application publishers/ connectors must operate in high availability (HA) and support built-in load balancing.	The application publishers/ connectors must operate in high availability (HA) and support built-in load balancing and there should not be any additional license cost linked with the addition of any number of publishers/ connectors throughout the project tenure. The license model for VPN/ZTNA will be purely based on proposed user license only.
12.	Functional & Technical Requirements VPN/ Zero Trust Network Access (Sr No. 46)	The solution must have the ability to universally define, deploy, and immediately enforce policies for all users, across all locations from a single console. The policy updation must be in real-time.	The solution must have the ability to universally define, deploy, and immediately enforce policies for all users, across all locations from a single console. The policy updation must be in real-time and there should not be any limitation in the number policies that can be created for ZTNA
13.	Functional & Technical Requirements Administration, Management & Reporting (Sr No. 70)	For advanced analytics and forensic purposes, the proposed solution must provide at least 90 days of globally correlated real-time interactive reporting for every web transaction.	For advanced analytics and forensic purposes, the proposed solution must provide at least 7 days of globally correlated real-time interactive reporting for every web transaction.
14.	Functional & Technical Requirements Cloud Based Secure Web Gateway/ Proxy (Sr No .17)	For effective utilization of the available Bank's network bandwidth, the proposed solution must provide the functionality for bandwidth caping based on users/ groups/ application accessed etc.	The clause stands removed.
15.	Functional & Technical Requirements Cloud Based Data Loss Prevention Solution	Additional clause	The proposed solution must have an inbuilt Incident Workflow Management for DLP events, and it should support the integration of such incident flows with Banks SIEM/ ITSM tools from Day1 without any additional license cost.
16.	Schedule of Events	4. Last date and time for Bid submission: Up to 4.00 PM on August 11, 2025 6. Date and Time of opening of technical bids : 4.30 PM on August 11,2025	4. Last date and time for Bid submission: Up to 4.00 PM on August 21, 2025 6. Date and Time of opening of technical bids : 4.30 PM on August 21,2025