NPCI/2024-25/PROC/258 Date: 30.05.2024.

Registered Office - 1001A, B Wing, 10th Floor, 'The Capital', Bandra Kurla Complex, Bandra (E), Mumbai - 400 051

Corrigendum-4

This is with reference to NPCI's RFP no. NPCI/RFP/2024-2025/IT/01 dated 06.05.2024. **Proposal for collocated DC facility for hosting NPCI Data Centre at Mumbai/Navi Mumbai for period of 5 years.** The prospective bidders may please note the following changes:

Sr. No.	Document Reference	Description	Amended RFP date vide Corrigendum -2	Amended RFP date vide Corrigendum -4
1	Section 1 - Bid Schedule and Address for Submission Sr. no. 6 Page no. 9	Last date and time for Bid Submission	31st May 2024, 18:00 Hrs	10th June 2024, 18:00 Hrs
2	Section 1 - Bid Schedule and Address for Submission Sr. no.8, Page no.9	Date and Time of Eligibility & Technical bid Opening	31st May 2024, 19:00 Hrs	10th June 2024, 19:00 Hrs

NPCI/2024-25/PROC/258 Date: 30.05.2024.

Sr. No.	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)	Revised Clause
1	8.37 Cyber Incident Reporting Clause for Vendors	37	1.1, 1.2, 1.3,1.4,1.5	Entire Cybersecurity related clause	Regarding the cyber incident reporting clause and the data protection clause, we would like to clarify that **our colocation service does not include any managed services of the customer's application, network, data or any other IT assets.** Therefore, the scope of the cyber security incident for us as the supplier is limited to the physical security of the data centre premises. We do not have any logical access to or control over the customer's information systems or data, so supplier is not responsible for any breach or unauthorized access that may occur at the customer's system. We request you to kindly remove this clause as this is more suitable for a managed hosting service provider or a cloud service provider.		The Service Provider acknowledges that the Government of India has declared the computer resources relating to certain products of NPCI, being Critical Information Infrastructure of NPCI and the computer resources of its associated dependencies to be protected systems for the purpose of the Information Technology Act, 2000. In this regard, the Service Provider agrees and undertakes to report to NPCI the occurrence of all Cyber Incidents (defined below). For the purposes of this clause / agreement, Cyber Incidents shall mean an attempted breach or breach as observed in the Information Security systems of the Service Provider and Operational Technology systems for the Colocation Data Centre and or any unauthorised access to or breach in the Information Technology-based systems of the Service Provider, as more specifically specified below: I. Targeted scanning or probing of critical networks or systems of service provider. II. Unauthorised access of Information Technology / Operational Technology systems or data. III. Defacement of service provider website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc. IV. Malicious code attacks such as spreading of Virus/Worm/Trojan/Bots/Spyware/ Ransomware/Crypto miners. V. Attack on servers such as database, mail, DNS and network devices such as routers VI. Identity theft, spoofing and phishing attacks. VII. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. VIII. Attacks or malicious/suspicious activities affecting systems/servers/networks/ software/applications related to Big Data, Blockchain, virtual assets, virtual asset exchanges, AI (Artificial Intelligence) & ML (Machine Learning), automation, robotics, etc. IX. Data breaches. X. Data leaks. XI. Unauthorised access to social media accounts. XII. Attacks or malicious or suspicious activities affecting cloud computing systems, servers, software, or applications. Systems of Operational Technology may include but not limited to following examples: i. Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs). ii. Remote Terminal Units (RTUs) iii. Human-Machine Interfaces (HMIs). iv. Safety Instrumented Systems (SIS). v. Sensors and Actuators. vi. Industrial Networks (Fieldbus and Industrial Ethernet). vii. Building Management Systems (BMS) & Energy Management Systems (EMS). viii. Environmental Monitoring Systems & Telemetry systems. ix. Utility Control Systems & Access Control Systems. 2. In the event the Service Provider finds any malware and/or if any Cyber Incident occurs on their Internal IT/OT systems, the Service Provider shall notify NPCI of the same, in writing and ensure the following: a) Cyber Incidents including malware related incidents should be reported within 24 hours of the detection of such incident. b) Communication should be sent to **csirt@npci.org.in.** c) The communication should be clear and concise, providing all the necessary information about such incident, including the steps that are being taken to address the issue and minimize any potential damage. d) The communication should clearly articulate about the impact it may have on NPCI, as well as any potential risks or vulnerabilities that may be exposed and perceived threats to the Service Provider's organization systems, data, or operations. e) It should also provide guidance on what steps the Service Provider is going to take to protect themselves from any potential threats or vulnerabilities that may arise because of the incident. 3. The Service Provider agrees that any failure to comply with the above-mentioned obligation will constitute a material breach of the Agreement/PO and NPCI will have the right in its sole discretion to terminate the Agreement/PO. 4. Additionally, NPCI has the right to impose penalty @ the rate of 1% of the total value of the [PO/Fees under the Agreement] for each event of failure of reporting a Cyber Incident by the Service Provider (as per clauses above) or claim a total amount of Rs. 50,000 from the Service Provider whichever is higher.

NPCI/2024-25/PROC/258 Date: 30.05.2024.

Sr. No.	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)	Revised Clause
2	8.38 Data Protection	38	1.1, 1.2, 1.3	Entire Data Protection clause	Since we are providing only colocation services, which includes physical space and Power as a service and **does not have access to any of the customer's IT setup or data, thus, this clause is not applicable to the Data center service provider.** We request you to kindly remove this clause as this is more suitable for a managed hosting service provider or a cloud service provider.		No change