CORRIGENDUM-III

TENDER NO. WTL/PAR/NEODBBACKUP/25-26/033 Dated 25.9.2025

Sl. No.	Section No.	Page No/ Clause No	Existing Criteria	New Criteria	Document to be submitted
1	SECTION – B: Eligibility Criteria – Capability	Page-10 New Clause	NA	CSP should have FIPS 140-level 3 compliant single tenant cloud managed self-serve provisioning HSM unit. Proposed HSM should be a managed service of same cloud service provider and should be able to provide availability of HSM within 1 hour, in case of any failure of HSM unit.	Valid copies of proof attested by authorized Bid signatory
2.	SECTION – B: Eligibility Criteria – Capability	Page-10 New Clause	NA	CSP should have native Threat Management service for proactive and reactive response (covering logs, malware protection, data breach threats like logging attempts, databases, security threat in container environments)	Valid copies of proof attested by authorized Bid signatory
3	SECTION – B: Eligibility Criteria – Capability	Page-10 New Clause	NA	CSP should have native Network Firewall with minimum 100 gbps throughput along with TLS 1.3 support for CDN, Load balancer and API gateway	Valid copies of proof attested by authorized Bid signatory
4	SECTION – B: Eligibility Criteria – Capability	Page-10 New Clause	NA	CSP must have capability to provide Object Storage with Redundancy and with Intelligent Tiering across availability zones with storage durability of 99.999999999%	Valid copies of proof attested by authorized Bid signatory
5	SECTION – B: Eligibility Criteria – Capability	Page-10 New Clause	NA	CSP must have Monitoring and Connectivity Services as below: a. Inspector service to manage and monitor vulnerability b. Native Cloud Security Posture Management (CSPM) service c. Cloud native API Gateway	Valid copies of proof attested by authorized Bid signatory

.