Tender for Supply, Installation and Maintenance of Data Center Components

Tender No. AEDC/DC-DR/ 2026-27/01, Date 13/03/2026

Assam Electronics Development Corporation Limited.
Bamunimaidan, Guwahati,
Assam, PIN-781021

Affix Court Fee Stamp of value Rs. 100.00 here

Section-1

Assam Electronics Development Corporation Ltd. (AMTRON)
Industrial Estate, Bamunimaidan
Guwahati - 781021

NOTICE INVITING TENDER ENQUIRY

Ref No. AEDC/DC-DR/2026-27/01 Dated. 13/03/2026

Assam Electronics Development Corporation Ltd (AMTRON) invites bids for "Supply of Red Hat Enterprise Linux for Virtual Data Centers" having technical specification as detailed below in relevant section.

The tender Document is available in https://amtron.in. Bidder are requested to check the website for amendments/corrigendum. Submission of bids shall be offline and to be submitted in the ***Drop Box as mentioned in below table.***

1.1 SCHEDULE OF TENDER

Tender No.	**AEDC/DC-DR/2026-27/01**
Scope of Work	Supply of items specified in this tender.
Name of the tender issuer	Assam Electronics Development Corporation Ltd.
Date of issue of tender document	**13-03-2026**
Last Date for Submission of Bids	All Tender Documents to be submitted in the Drop Box available at 3rd Floor, AMTRON Data Center Building, A.E.D.C. Ltd., Industrial Estate, Bamunimaidan, Guwahati, PIN-781021, by **3:30 PM, 10-04-2026**.
Date of Opening of Technical & Financial Bids	**10-04-2026 at 03:30 PM**
Place of Submission & Opening of Bids	3rd Floor, AMTRON Data Center, A.E.D.C. Ltd.
Address for Communication	Managing Director Assam Electronics Dev. Corporation Ltd., Industrial Estate, Bamunimaidan, Guwahati – 781021, Assam
Phone No. for Communication	+91-9864917608
e- mail ids	mdc@amtron.in

1.1.2. Tender Processing Fee:

A non-refundable fee of Rs 10,000/- (Ten Thousand) shall be made towards the cost of tender processing fee through any bank in favour of Managing Director, Assam Electronics Development Corporation Limited.

1.1.3 Bid Security/Earnest Money Deposit

The bid document must be accompanied by the Earnest Money Deposit of Rs. 10,00,000.00 (Rupees Ten Lakh Only) through any bank in the form of DD/BG in favour of Managing Director, Assam Electronics Development Corporation Limited.

PART I - TECHNICAL BID

1.2 Pre-Qualification Criteria:

i. The Bidder should be a Company having its registered Office in Assam.
   a. Certificate of Incorporation/Trade License to be provided.
   b. GST Registration and PAN Card to be furnished.
   c. Profile of Company – **Form C**

ii. Unpriced, complete and correct BOQ consisting of OEM Part Codes to be submitted.

1.3 Scope of work:

Supply: The bidder should supply the items as per the Bill of Materials (BOM) below. All goods need to be supplied F.O.R. Guwahati.

BOM:

SL	Description	Qty	Unit
1	Rack Server (type-1)	12	nos.
2	Rack Server (type-2)	17	nos.
2.1	Rack Server (type-3)	1	nos.
2.2	Rack Server (type-4)	1	nos.
2.3	Rack Server (type-5)	2	nos.
3.1	Unified Storage (type-1)	1	nos.
3.2	Object Storage (type-1)	1	nos.
4.1	Unified Storage (type-2)	1	nos.
4.2	Object Storage (type-2)	1	nos.
5	SAN Switch (type-1)	2	nos.
6	SAN Switch (type-2)	2	nos.
7	Virtual Tape Library	1	nos.
8	Web Application Firewall	2	nos.
9	Other Software	1	lot
10	Out of Band Management Switch (Type-1)	1	nos.
11	Out of Band Management Switch(Type-2)	2	nos.
12	Core/Spine Switch (Type-1)	2	nos.
13	Core/Spine Switch (Type-2)	2	nos.
14	Server/Leaf Switch (Type-1)	2	nos.
15	Server/Leaf Switch (Type-2)	2	nos.
16	Next Generation Firewall	2	nos.
17	Security Incident and event Management tools (SIEM)	1	lot
18	Monitoring System	1	lot
19	KVM with KMM Switch (Type-1)	1	nos.
20	KVM with KMM Switch (Type-2)	1	nos.
21	Security Operations Center (SOC)	1	lot
22	Venerability assessment tools	1	lot
23	API monitoring solution	1	lot

SL	Description	Qty	Unit
24	Clientless Web SSL VPN	1	lot
25	Windows Server Remote Desktop Environment for 150 user	1	Lot

Sd/

Date: 13-03-2026
Guwahati

Managing Director
AEDC Ltd. (AMTRON)

For further details and Tender Documents please visit www.amtron.in

1.4. Minimum Technical Specifications *(Proposed Specification and Compliance (Yes/No) should be filled by the Bidder for all the tables 6.3.1 till 6.3.23)*

1.4.1 Rack Server (type-1 & type-2) (SL 1 & SL 2)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1.	Make		
2.	Model		
3.	Physical Cores- minimum 320 nos. latest generation processor minimum 2.0GHz base frequency		
4.	Each server should have minimum 4TB Memory		
5.	2 x 1TB SSD offered in Minimum RAID configuration		
6.	• Each server should have 4 x 25 Gbps (minimum) for Ethernet ports populated with 4 (four) numbers of 25Gbps multimode transceivers. • Each server should have 2x32Gbps FC ports populated with 2 nos. of 32Gbps transceivers • Each server to be supplied with 6 nos. of (Optical Multimode) OM3/OM4 multimode patch cords of appropriate length for connecting to proposed Server Switches and SAN Switches.		
7.	Dedicated out of band management port from Day1.		
8.	Proposed server should have hot swappable redundant power supply and fans to meet 100% workload with proposed components.		
9.	Server should support cloud and container platforms.		
10.	Rack mountable with rail kit.		
12	Server Form Factor should be 1 (one) / 2 (Two) RU to optimize the Rack space utilization and cost at SDC and DR locations		
11.	Standard Compliance Required - UL, FCC/BIS & RoHS		

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
3.	Physical Cores- minimum 320 nos. latest generation processor minimum 2.0GHz base frequency		
4.	Each server should have minimum 4TB Memory		
5.	2 x 1TB SSD offered in Minimum RAID configuration		
6.	• Each server should have 4 x 25 Gbps (minimum) for Ethernet ports populated with 4 (four) numbers of 25Gbps multimode transceivers. • Each server should have 2x32Gbps FC ports populated with 2 nos. of 32Gbps transceivers • Each server to be supplied with 6 nos. of (Optical Multimode) OM3/OM4 multimode patch cords of appropriate length for connecting to proposed Server Switches and SAN Switches.		
7.	Dedicated out of band management port from Day1.		

8.	Proposed server should have hot swappable redundant power supply and fans to meet 100% workload with proposed components.		
9.	Server should support cloud and container platforms.		
10.	Rack mountable with rail kit.		
12	Server Form Factor should be 1 (one) / 2 (Two) RU to optimize the Rack space utilization and cost at SDC and DR locations		
11.	Standard Compliance Required - UL, FCC/BIS & RoHS		

1.4.2. Rack Server (Type-3 & Type 4) (SL 2.1 & SL 2.2)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1.	Make		
2.	Model		
3.	Physical Cores- 12 nos. latest generation processor minimum 2.0GHz base frequency		
4.	Each server should have minimum 512 GB Memory		
5.	3 x 1TB SSD offered in Minimum RAID configuration		
6.	• Each server should have 4 x 25 Gbps (minimum) for Ethernet ports populated with 4 (four) numbers of 25Gbps multimode transceivers. • Each server should have 2x32Gbps FC ports populated with 2 nos. of 32Gbps transceivers • Each server to be supplied with 6 nos. of (Optical Multimode) OM3/OM4 multimode patch cords of appropriate length for connecting to proposed Server Switches and SAN Switches.		
7.	Dedicated out of band management port from Day1.		
8.	Proposed server should have hot swappable redundant power supply and fans to meet 100% workload with proposed components.		
9.	Server should support cloud and container platforms.		
10.	Rack mountable with rail kit.		
12	Server Form Factor should be 1 (one) / 2 (Two) RU to optimize the Rack space utilization and cost at SDC and DR locations		
11.	Standard Compliance Required - UL, FCC/BIS & RoHS		

1.4.3 Rack Server (type-5) (SL 2.3)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1.	Make		
2.	Model		
3.	Physical Cores- 12 nos. latest generation processor minimum 2.0GHz base frequency		
4.	Each server should have minimum 512 GB Memory		
5.	3 x 1TB SSD offered in Minimum RAID configuration		
6.	• Each server should have 4 x 25 Gbps (minimum) for Ethernet ports populated with 4 (four) numbers of 25Gbps multimode transceivers. • Each server should have 2x32Gbps FC ports populated with 2 nos. of 32Gbps transceivers • Each server to be supplied with 6 nos. of (Optical Multimode) OM3/OM4 multimode patch cords of appropriate length for connecting to proposed Server Switches and SAN Switches.		
7.	Dedicated out of band management port from Day1.		
8.	Proposed server should have hot swappable redundant power supply and fans to meet 100% workload with proposed components.		
9.	Server should support cloud and container platforms.		
10.	Rack mountable with rail kit.		
12	Server Form Factor should be 1 (one) / 2 (Two) RU to optimize the Rack space utilization and cost at SDC and DR locations		
11.	Standard Compliance Required - UL, FCC/BIS & RoHS		

1.4.4 Unified Storage (type-1 & type-2) (SL 3.1 & SL 4.1)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1	Make		
2	Model		
3	The proposed storage solution shall provide a highly available, scale-out architecture with no single point of failure, supporting active-active controllers or functionally equivalent mechanisms. The solution shall allow seamless, non-disruptive scaling of capacity and performance and shall be capable of scaling to a minimum of 1000 TB usable capacity.		
4	RESTful and S3-compatible APIs for management and automation.		

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
5	Should have Container Storage Interface (CSI) feature from day one. Offered Storage shall be integrated with proposed container and virtualization platform.		
6	The proposed storage solution shall provide a minimum of **150 TB usable capacity** using enterprise-grade NVMe/SSD drives. The solution shall include sufficient hot spare capacity to ensure data protection and high availability, with a minimum of two (2) hot spare drives or equivalent redundancy mechanism. The drive capacities offered shall be of appropriate enterprise-class sizes to meet the required usable capacity and performance. Each NVMe/SSD drives should be minimum 12 TB or higher.		
7	The proposed storage solution shall support a unified architecture capable of providing block (iSCSI, FC, NVMe-oF), file (NFS and SMB/CIFS), and object storage services with S3-compatible APIs. Object storage functionality shall be provided as a native or tightly integrated component of the proposed solution, fully supported and managed through the same management framework, without reliance on separate third-party hardware platforms.		
8	Should be supplied with at least 256GB Memory for Read and write operations.		
9	The array must keep write cache persistent during fault conditions.		
10	Should be supplied with - 4x100Gbps Ethernet ports populated with 100Gbps multimode transceivers and 4 nos. of MPO cables of length 15 meters. AOC/DAC (cables) may also be proposed to achieve the 100Gbps uplinks to proposed Server Switches. - 4X32Gbps FC Ports populated with 32Gbps transceivers and 4 nos. of OM3/OM4 cables of appropriate length to connect to proposed SAN Switches.		
11	The proposed array should support QoS feature to limit the amount of IOPS or bandwidth (MB/s) that a particular application can drive on the array.		
12	The Storage array must provide end-to-end data protection using industry standard mechanism such as parity checking, checksum etc.		
13	The Storage should be offered with highly available configuration with No Single Point of Failure (NSPoF) architecture and redundancy features at all levels of Hardware and Software (such as controllers, hot swap power supplies, PDUs, cache, links between subsystems etc.)		

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
14	The Storage array must provide multiple levels of access control including role-based security and auditing capability.		
15	The storage array should support connectivity to current version of OS Platforms like Linux, Windows etc.		
16	Storage subsystem shall be supplied with Thin Provisioning, Snapshot, De-duplication, Compression, Performance Monitoring, and Quality of service on day 1.		
17	In the event of unplanned power failure, data in the cache should be safely de-staged to the disks to protect data from loss.		
18	The storage system should support non-disruptive field replacement capabilities for components like Disk Drives, Disk connections, power supplies, controllers etc.		
19	The Storage array should support continuous system monitoring, advanced remote diagnostics, availability and reliability.		
20	The storage should be configured with easy to manage, simple integrated user interface for distributed storage environments. A single sign-on centralized console should have dashboards for at-a- glance management and reporting and other functions like configuration monitor and manage. Performance monitoring should be provided to analyze the performance data.		
21	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives. Storage should be provided with File level retention and 256 Bit encryption.		
22	Storage shall support integration with LDAP and Active Directory.		
23	The proposed array should be supplied with native Storage management software with GUI capable of generating customized reports, real time monitoring, historical performance data for analysis and trending, capacity utilization monitoring.		
24	Storage shall support CLI, Web and Rest API based management of storage array		
25	Total Rack Unit of the proposed solution.Rack mountable with rail kit		
26	Management– Out of Band Management with license/feature ready.		
27	Standard Compliance Required - UL, FCC & RoHS		

6.3.5 Object Storage (type-1 & type-2) (SL 3.2 & SL 4.2)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1	Make		
2	Model		
3	Scale-out architecture seamless expansion of capacity and performance without service disruption. Minimum scalability up to 2000TB usable capacity.		
4	RESTful and S3-compatible APIs for management and automation.		
5	Should have Container Storage Interface (CSI) feature from day one. Offered Storage shall be integrated with proposed container and virtualization platform.		
6	The storage system shall deliver a minimum of **150 TB usable capacity** using enterprise NVMe/SSD drives, with at least two hot spares configured for high availability. Equivalent or higher-capacity configurations shall be acceptable. Each NVMe/SSD drives should be minimum 12 TB or higher.		
7	Object storage must be natively integrated by the same OEM platform, not via third-party OEM or separate stack.		
8	The solution should support Read and Write throughput of 500MB/s and 400MB/s.		
9	Should be supplied with - 4x25Gbps Ethernet ports populated with 4 nos. of 25Gbps multimode transceivers and 4 nos. of MPO cables of length 15 meters. AOC/DAC (cables) may also be proposed to achieve the 25Gbps uplinks to proposed Server Switches. Equivalent or higher-capacity connectivity shall be acceptable.		
10	Total Rack Unit of the proposed solution. Rack mountable with rail kit		
11	Management– Out of Band Management with license/feature ready.		
12	Standard Compliance Required - UL, FCC & RoHS		
13	Must support S3 Object Lock (Compliance Mode & Governance Mode).		
14	Must support S3 Versioning and Lifecycle Policies (automatic tiering, archival, expiration).		
15	Must support S3 Cross-Region / Cross-Site Replication.		
16	Must support S3 Select for optimized object-level querying (if supported by OEM).		
17	Must support multi-tenant S3 buckets with quota, isolation, and security policies.		
18	Must support S3-compatible encryption mechanisms: SSE- S3, SSE-C, and Client-side encryption.		
19	Must support S3 event notifications (webhooks, AMQP, Kafka, or equivalent open-standard eventing).		

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
20	Object storage cluster must support erasure coding for data durability.		
21	Minimum durability requirement:≥ 11 nines (99.999999999%) or OEM equivalent durability architecture.		
22	Metadata operations must be distributed without single bottleneck (strong consistency preferred).		
24	Must support seamless tiering to cloud (AWS S3, Azure Blob, GCP) using standard S3 API without vendor lock-in.		
25	Must support WORM (Write Once Read Many) retention with audit logging.		
26	Must support encryption of data in transit using TLS 1.2/1.3.		
27	Must support multi-site active-active or active-passive S3 topology for DR.		

6.3.6 SAN Switch (type 1 & type 2) (SL-5 & 6)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1.	Make		
2.	Model		
3.	The fibre channel switch must be rack mountable.		
4.	The switch to be configured with minimum of 32 ports with 32Gbps FC ports configuration backward compatible to 16Gbps.		
5.	All 32 nos. of FC ports for device connectivity should be 32 Gbps auto- sensing Fiber Channel ports populated with 32 nos. of 32Gbps FC Transceivers and Fiber Patch cords.		
6.	The switch must have hot-swappable redundant power supply from day 1.		
7.	The switch must be able to support non-disruptive software upgrade.		
8.	The switch must be able to support stateful process restart.		
9.	The switch must be capable of creating multiple hardware- based isolated Virtual Fabric instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers etc. for added scalability and resilience.		
10.	The switch must be capable of supporting hardware- based routing between Virtual Fabric instances.		
11.	The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances.		
12.	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers.		
13.	The switch must support hardware ACL based Port Security, Virtual SANs (VSANs), and Port Zoning.		
14.	The switch must support Smart Zoning such that the entries in the TCAM is significantly reduced and therefore increasing the overall scalability of the SAN Fabric.		
15.	The switch must support Power-On Auto Provisioning and Quick Configuration Wizard for simplified operations.		
16.	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.		
17.	The switch must support routing between Virtual Fabric instances in hardware.		
18.	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.		
19.	ID and Destination ID. The support for load balancing utilizing the Exchange ID must also be supported.		

20.	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.		
21.	The switch must be capable of discovering neighboring switches and identify the neighboring Fiber Channel or Ethernet switches.		
22.	The switch should support IPv6.		
23.	Rack mountable with rail kit		
24.	Standard Compliance Required - UL, FCC & RoHS		

6.3.7 Virtual Tape Library (SL 7)

Sl. No	Technical Parameter	Proposed Specification	Compliance (Yes/ No)
1	**Make**		
2	**Model**		
3	System must support modular, scale-out architecture allowing non-disruptive capacity and performance expansion.		
4	Must support integration with at least three industry- standard enterprise backup software platforms (ISVs) using open protocols/APIs.		
5	Minimum usable capacity of 300 TB (native, before deduplication). And Expandable to at least 1 PB usable capacity (native).		
6	Must support direct cloud/object storage tiering without requiring an external gateway.		
7	Operating system must be stored on isolated media, separate from backup data.		
8	Must support factory-configured RAID-6 or equivalent dual-parity protection.		
9	Must support both VTL over Fibre Channel and NAS (NFS/SMB) protocols.		
10	Ability to create full backup copies to external devices while retaining local copy.		
11	Must support creation of at least 128 virtual tape libraries.		
12	Must support granular restore directly from disk-based backups.		
13	Inline deduplication with bandwidth-efficient replication (transmit only unique data).		
14	Must support both source-side and target-side deduplication with at least 3 backup software integrations.		
15	Minimum host I/O: 2×10GbE and 4×32G FC including required 10Gbps SFPs (multimode)		
16	FC connectivity (direct-attach or via SAN) with support for source- and target-side dedupe workflows		
17	Must support AES-256 data-at-rest encryption and TLS/SSL encryption for data-in-transit.		
18	High-risk administrative operations must require two-person approval.		
19	Dual-authorization enforced at the appliance level, independent of backup software		
20	Must support secure data sanitization/erase compliant with industry standards.		

21	System must support sustained ingest throughput of at least 100 TB per hour.		

6.3.8 Web Application Firewall Solution (SL 8)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1	**Make**		
2	**Model**		
3	The proposed appliance should have all integrated Web Application Firewall features from day 1.		
4	The appliance should have certification from any globally recognized independent security testing laboratory (e.g., ICSA, Common Criteria, EAL, or equivalent) and must protect against all OWASP Top 10 attack categories.		
5	The proposed appliance should provide minimum 10 Gbps Layer 7 throughput.		
6	The proposed appliance should have minimum: - 4xRJ45 Copper Ports - 2 x SFP+ ports populated with 2 nos. of l0Gbps SFP+ multimode transceivers. Layer 4 connections per second:5,00,000 Layer 7 connections per second:2,00,000		
7	16GB RAM		
8	20000: SSL connections/transactions per second TLS 1.3 Support from day 1		
9	Appliances should support 5 million SYN/sec as part of DDoS solution. The DDoS solution may be inbuilt or separate appliances may be proposed to meet the requirement.		
10	The proposed appliance should have capability to run in Virtualized as well as Standalone mode.		
11	The proposed device should be able to be partitioned into3 minimum Virtual Instances from Day 1		
12	The proposed solution should detect, and block tampered web pages automatically/promptly.		
13	WAF should have the flexibility to be deployed in Reverse proxy.		
14	The WAF should support below mode a) Active-Active, b) Active-Passive		
15	The device should support for IPv4 and IPv6 traffic		
16	Auto Policy Optimization Zero Day Attack Blocking. Auto Discovery c) The solution should protect from “Zero-day” attacks.		
17	Should support customization report, periodic reports from Day 1 Should support real time and historical Security Reporting from Day 1		

18	The solution should comply with globally recognized safety and electromagnetic compatibility standards such as UL/IEC/EN for safety and FCC/CE/ICES/Equivalent for EMC.		
19	Must support **API Security**, including protection for REST, XML, SOAP, JSON, GraphQL APIs.		
20	Must support **Bot Management** including detection of automated traffic, rate control, CAPTCHA enforcement, device fingerprinting.		
21	Must support **Web Application Behavioral Learning** for anomaly detection without signatures.		
22	Must support **Signature-based + Heuristic-based + Behavioral-based** detection engines.		
23	Must support **Full SSL Inspection** (Inbound & Outbound) with hardware/software acceleration.		
24	Must support **Content Caching**, **URL Rewriting**, and **Header Manipulation** for application optimization.		
25	Must support **Protection for File Upload Vulnerabilities**, including malware scanning integration.		
26	Must support **Advanced Rate Limiting / Throttling** policies per URL/IP/Session/API Key.		
27	Should integrate with **SIEM** solutions (Syslog, CEF, LEEF, JSON) from Day 1.		
28	Must provide **Role-Based Access Control (RBAC)** and **multi-factor authentication** for administrative access.		
29	Must support **Configuration Backup/Restore**, **Version Control**, and **Change Audit Logs**.		
30	WAF must support deployment in **On-Prem**, **Private Cloud**, **Public Cloud**, and **Hybrid** environments.		

6.3.9 Other software (SL 9)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/No)
Virtualization Software			
1	**Make**		
2	**Model**		
3	Should support multiple industry-standard OS distributions (Windows Server, major Linux distributions)		
4	Design, supply, installation, configuration, and commissioning of the solution across DC, DR and multi-site on x86_64 servers and shared storage.		
5	Should have the capability for creating VM templates to provision new servers		
6	Should support VM snapshots to revert back to an older state, as and when required.		
7	Should have live Virtual Machine migration between two or more servers in a cluster without downtime.		
8	Virtualization software shall have High Availability capabilities for the virtual machines. The feature should be independent of Operating System Clustering and should work with FC/iSCSISAN and NAS shared storage.		
9	Should provide the capability to live migrate the Virtual Machines.		
10	Should allow for creating virtual Networks that connect virtual machines.		
11	Should provide a Web Based Virtualization administrator portal with a graphical management mode for administrators to manage virtual machines, templates, storage, clusters, and Data Centers.		
12	Should provide Single-view centralized control of Host and VM system monitoring and management.		
13	It should able to provide VM level isolation for better security.		
Cloud Management & Orchestration Solution			
14	Design, supply, installation, configuration, and commissioning of the solution across DC/DR and/or multi-site on x86_64 servers and shared storage.		
15	Air-gapped content mirror support for container images, OCI artifacts, OS packages		
16	The solution should deliver platform add-ons, private container registry, GitOps, CI/CD, service mesh, serverless, observability, logging, alerting, audit, and policy controls.		
17	The solution should provide Multi-zone, cluster design, hypervisors, virtual network for L3/L4, Software load balancing, VLAN/VXLAN networking, optional SR-IOV/DPDK, storage via NFS/iSCSI/FC/NVMe-TCP.		
18	The solution should provide Automated creation/upgrade of upstream Kubernetes clusters, cluster HA, and lifecycle management.		
19	The solution should provide CNCF-compliant container registry with vulnerability scanning, GitOps-supported deployment engine, standards-based CI/CD pipeline, industry-standard service mesh, and serverless + event- driven autoscaling capabilities.		

20	The solution should provide an industry-standard centralized logging stack, OIDC-compliant SSO provider, policy engine compatible with admission control frameworks, and hardware- assisted or kernel-isolated container runtime.		
21	The solution should provide CPU pinning, hugepages, NUMA awareness, live migration where supported.		
22	The solution should provide Source NAT, static NAT, port forwarding, HA for Network Gateways, API/LB VIPs.		
23	The solution should provide L4/L7 ingress for tenant applications and for Kubernetes control-plane endpoints.		
24	The solution should provide Storage via NFSv4, iSCSI, FC, or NVMe-TCP, Storage should support for templates/ISOs, volume snapshots, templating, and cloning.		
25	The solution should provide Management servers in HA, database HA/replication, hypervisor HA, VM anti-affinity.		
26	The solution should provide create/resize/upgrade clusters, control-plane≥3 nodes with rolling upgrades and surge capacity, worker rolling upgrades respecting Pod Disruption		
27	The solution should support CNCF-compliant CNI plugins, standards-based DNS service, industry-standard ingress controllers, and CSI-compatible storage integrations.		
28	The solution should provide Horizontal Pod Auto scaler (CPU/Memory), Vertical Pod Auto scaler for rightsizing		
29	The solution should support a CNCF-compliant serverless framework with scale-to-zero capability.		
30	The solution should provide a runtime class supporting lightweight VM-based isolation for containers.		
31	The solution should provide virtualization layer for VM workloads with hardware offload where available (CPU pinning, huge pages, NUMA awareness, live migration where supported).		
32	The solution should provide container orchestration layer offering cluster lifecycle (create/resize/upgrade), high		
33	The solution should provide control plane high availability with odd-member quorum and resilient data store, workers		
34	The solution should provide standards-based container runtime and image format (OCI) with admission controls and runtime classes for isolation.		
35	The solution should provide networking via an industry- standard container networking interface with support for Network Policies, egress controls, and dual-stack IPv4/IPv6.		
36	The solution should provide service exposure via ingress/egress controllers with TLS termination, SNI, and certificate rotation.		
37	The solution should provide storage via an industry-standard container storage interface and support for dynamic provisioning, snapshots, and clones.		
38	The solution should provide auto scaling: Horizontal (workload metrics), Vertical (rightsizing recommendations and enforcement), and event-driven auto scaling using custom/external metrics.		
39	The solution should provide support for Vmware, Xen, KVM etc, optional enablement for additional supported hypervisors.		
40	The solution should provide live migration within a cluster, maintenance mode with evacuation, host fencing and automated recovery where supported.		

41	The solution should provide compute offerings define vCPU, RAM, CPU cap/weight, CPU overcommit ratios, and storage tags, support for host and VM affinity/anti-affinity rules.		
42	The solution should provide support different networking models, Multiple network tiers, network ACLs.		
43	The solution should provide segmentation via VLAN and/or VXLAN, dual-stack IPv4/IPv6 (including IPv6 addressing on guest networks) where feasible.		
44	The solution should provide support for strong tenancy, Projects for cross-account collaboration with isolated resource accounting.		
45	The solution should provide role-based access control (RBAC) with predefined and custom roles, API/secret key model for programmatic access, audit logging of administrative actions.		
46	The solution should provide support for project/account quotas for instances, vCPUs, RAM, volumes, snapshots, public IPs, and networks.		
47	The solution should provide project-level resource limits, alerting when thresholds are reached, capacity planning dashboards.		
48	The solution should provide metrics for hosts, clusters, storage, with standard time-series/visualization stacks.		
49	The solution should generic platform with run books/playbook, safe delegation, job scheduling, and cross-tool integrations.		
50	The solution should generic controller for configuration and application automation using declarative playbooks/runbook/roles.		
51	The solution should generic, multi-tenant portal providing department portals, catalogs from private-cloud usage.		
52	The solution should project/workspace model with role-based isolation; folders and naming policies.		
53	The solution should job authoring with steps, options (typed/validated), secured parameters, and reusable templates.		
54	The solution should target hosts prepared by automation: OS hardening, time sync, required kernel/modules/sysctl, swap disabled where required, firewall rules aligned with		
55	The solution should OS Operations: patching, reboot server, user & sudo management, SSH key rotation, time/NTP sync.		
56	The Entire solution should include minimum 100 physical severs(with each server specifications as minimum 320 physical cores)		

6.3.10 Out of Band Management Switch (Type-1 & Type-2) (SL 10 & SL 11)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1.	Make		
2.	Model		
3.	**Architecture**: 1U Rack-mountable Layer-2 switch with dual redundant power supply from day one. Minimum **24×1G RJ45 ports** and **2×1G SFP uplink ports** populated with **2×1G multimode SFP transceivers** and matching fiber patch cords. Minimum **24 Gbps switching capacity**.		
4.	**Layer 2 Features:** Support for IEEE 802.1Q VLANs, 802.1d STP, 802.1w RSTP, 802.1s MSTP, 802.3ad LACP. Port mirroring. Broadcast/multicast/unknown unicast storm control. Jumbo frame support. Private VLAN. Support minimum **16K MAC addresses**.		
5.	**Security:** Support for Advanced /Extended ACLs, RADIUS/ TACACS for authentication, SSHv2 for secure management, DHCP snooping, Port security.		
6.	**Management & Maintenance:** Web-based GUI, CLI via console, SSH, Telnet (optional), FTP/TFTP for file transfer, SNMP v1/v2c/v3, RMON or equivalent monitoring capabilities, and NTP for time synchronization.		
7.	Bidder shall include any additional accessories, modules, cables, or components required to make the solution fully functional.		
8	The switch operating system/firmware must be **developed, supported, and provided directly by the same OEM** as the switch hardware (no third-party OS).		
9	Certifications: Compliance with **CE or equivalent**, **RoHS**, **Safety standards (UL/EN/IEC/BIS)**, and **Electromagnetic compliance: TEC Class A**.		

6.3.11 Core/Spine Switch (SDC) (Type-1 and Type-2) (SL 12 and SL 13)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1.	Make		
2.	Model		
3.	Architecture– Single Switch/ modular switch. The switch should have: • System Memory (RAM) – 16GB or higher • Packet buffering capacity sufficient to support enterprise data-centre workloads (minimum equivalent of 32 MB or higher), irrespective of buffer architecture (shared or dedicated) • N+1 redundant hot-swappable AC Power Supply & hot-swapable fans • Power cables should be C13/C14 of minimum 3m length.		

4.	The switch should Rack Mountable.		
5.	The switch should have minimum 6.4Tbps or higher switching capacity providing non-blocking performance.		
6.	The switch should have - 32 nos. of 100Gbps ports of which - • 8 ports to be populated with 100Gbps multimode transceivers (MPO type) with equal nos. of MPO cables (15m length). • 12 active optical/direct attached cables of length 10 meters or higher offering 100Gbps each. • 4x40Gbps dedicated uplink ports populated 4x40Gbps multimode transceivers and optical cables. (Breakout cables are not allowed to meet 40Gbps or 100Gbps ports) • Console Port • Out-of-band Management Interface • Multimode MPO Patch Cord/cables as per design requirement.		
7.	Native dual-stack IPv4/IPv6 support from day one		
8.	**Layer-2 Features:** Support for 802.1p, 802.1Q VLAN, MSTP, flow control, LACP, port mirroring, traffic analytics (NetFlow/sFlow/jFlow/equivalent), storm control, UDLD/DLDP or equivalent, jumbo frames, Private VLAN, 64K MAC addresses, up to 64 MST instances, and 4000 VLANs.		
9.	Layer-3 Features: Static routing, DHCP, OSPFv3, IS-IS (v4/v6), BGPv4, PBR, dual IPv4/IPv6, VRRP or equivalent FHRP, graceful restart for OSPF, IS-IS, BGP, EVPN, VXLAN routing, ECMP, VRF, and Segment Routing (IPv4/IPv6).		
10.	**Security feature from day 1-** • Layer 3 and Layer 4 ACL for both IPv4 and IPv6 • MAC ACL • RADIUS / TACACS • Secure shell (SSHv2) • DHCP snooping		
	• Port security • Role Based Access Control • MACsec on all ports. • IP source guard		
11	Switch shall support application traffic visibility using standard flow-based monitoring (NetFlow/IPFIX/sFlow) and open-standards streaming telemetry.		

11.	**Management:** CLI via console, SSH, optional Telnet, FTP/TFTP, **SNMP v1/v2c/v3**, RMON/equivalent, NTP, **OpenConfig/YANG-based model-driven APIs**, and IPv6-enabled management interface.		
13.	**Certification** Must comply with CE or equivalent, RoHS, UL/EN/IEC/BIS safety standards, and FCC Class A / TEC Class A EMC standards.		
14	Switch OS/firmware must be developed and supported by the same OEM as the hardware (no third-party OS).		

6.3.12 Server/Leaf Switch (type-1 & type-2) (SL 14 & 15)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/ No)
1.	Make		
2.	Model		
3.	Architecture– Single/modular Switch The switch should have: • RAM –16GB or higher • Buffer– 32MB • N+1 redundant hot-swappable AC Power Supply & hot-swapable fans • Power cables should be C13/C14 of minimum 3m length.		
4.	The switch should Rack Mountable.		
5.	The switch should have minimum 3.2Tbps or higher switching capacity providing non-blocking performance.		
6.	The switch should have - • 44x25Gbps ports of which 44 ports to be populated with 25Gbps multimode transceivers and equal nos. of OM3/OM4 cables (5m length). • 4X10Gbps ports to be populated with 4 nos of 10Gbps multimode transceivers and cables. • 8x100Gbps dedicated uplink ports populated 4x100Gbps multimode transceivers and equal nos. of MPO cables (15m or higher length) (Breakout cables are not allowed to meet 10Gbps or 100Gbps ports) • Console Port • Out-of-band Management Interface • Multimode MPO Patch Cord/cables as per design requirement.		
7.	Native **dual-stack IPv4/IPv6 support** from day one		

8.	Layer-2 Features: Support for 802.1p, 802.1Q VLAN, MSTP, flow control, LACP, port mirroring, traffic analytics (NetFlow/sFlow/jFlow/equivalent), storm control, UDLD/DLDP or equivalent, jumbo frames, Private VLAN, 64K MAC addresses, up to 64 MST instances, and 4000 VLANs.		
9	**Layer 3/Routing features from day-1:** • Support for Static Routing • DHCP Server/Relay/Client functionality • Support for OSPFv3, IS-IS (IPv4 & IPv6), and BGPv4 • Policy-Based Routing (PBR) • Dual-stack IPv4/IPv6 routing • First Hop Redundancy Protocol (FHRP) such as VRRP or equivalent for IPv4 & IPv6 • Graceful Restart for OSPFv3, IS-IS (IPv4/IPv6) and BGPv4 • EVPN capabilities • VXLAN Routing support • ECMP multipath routing • Support for VRF (Virtual Routing & Forwarding) • Segment Routing for IPv4 and IPv6		
10	**Perpetual Security feature license-** • IPv4/IPv6 Layer-3 and Layer-4 ACLs • MAC-based ACLs • Support for RADIUS & TACACS+ authentication • Secure Shell (SSH v2) for secure management access • DHCP Snooping • IEEE 802.1X port-based network access control • MACsec encryption available on all data ports • Role-Based Access Control (RBAC) • IP Source Guard for preventing IP spoofing		
11	Switch shall support application traffic visibility using standard flow-based monitoring (NetFlow/IPFIX/sFlow) and open-standards streaming telemetry.		
11	**Management:** CLI via console, SSH, optional Telnet, FTP/TFTP, **SNMP v1/v2c/v3**, RMON/equivalent, NTP, **OpenConfig/YANG-based model-driven APIs**, and IPv6-enabled management interface.		
12	Must comply with CE or equivalent, RoHS, UL/EN/IEC/BIS safety standards, and FCC Class A / TEC Class A EMC standards.		

6.3.13 Next Generation Firewall (SL 16)

Sl. No	Minimum Specification	Proposed Specification	Compliance (Yes/no)
1	**Make**		
2	**Model**		
3	Firewall must include integrated security services: Anti-Malware, IPS, Application Visibility & Control, URL Filtering, Botnet Protection, and Sandboxing.		
4	Minimum 10 Virtual Firewall instances supported from day one.		
5	Support for standards-based SNMP v2c and SNMP v3.		
6	Support for standard NAT modes: 1:1, 1:Many, Many:1, Many:Many, and Overlapping/Transparent NAT.		
7	The Firewall should be minimum 100 Gbps of stateful firewall throughput. (for east west traffic).		
8	Minimum 500000 Concurrent HTTP/TCP Connections/sec from day 1		
9	Minimum 50000000 Concurrent Connections.		
10	Next Generation Firewall throughput of minimum 25Gbps (enabling Firewall, IPS and Application Control feature) from day one. (for internet bound traffic).		
11	Each firewall should have a minimum • 8 x 100Gbps ports populated with 8 nos. of 100Gbps multimode transceivers and equal nos. of MPO cables of length as per design requirement. • Additional 2 x 10Gbps ports populated with 2 nos. of 10Gbps multimode transceivers and cables. • Transceivers should be from same OEM as that of Firewall. Bidder may propose equal nos. of Direct Attach Cables/Active Optical Cables of same OEM as that of firewall.		
12	• Multi-core processor for threat analysis • 64 GB system memory from day one.		
13	Support standards-based authentication mechanisms including LDAP, RADIUS, Active Directory, and PKI certificate-based authentication.		
14	Standards-based IPS supporting IPv4/IPv6 inspection and adaptive DDoS and DoS protection with automated thresholding.		
15	Should have integrated Application control solution & should have Application identification engine supporting≥3000 applications using signature and behavioral analysis, independent of ports.		
16	Integrated Anti-Malware engine with antivirus, botnet detection, and spyware protection.		

17	Full security subscription bundle (Antimalware, IPS, Application Control, URL Filtering, Botnet protection, Sandboxing) included from day one.		
18	The firewall shall have Internet Protocol Security (IPSec) & SSL VPN (minimum 2000 User).		
19	Support for site-to-site VPN architectures including hub- and-spoke and full-mesh.		
20	Support for industry-standard encryption algorithms including AES-128/192/256 and 3DES.		
21	Support for modern hash/authentication algorithms such as SHA-1 and SHA-2 family.		
22	Support for centralized management, centralized logging, and comprehensive audit trail.		
23	5-years IPS, Application Control, Anti-Malware, Sandboxing & Anti-Bot subscription		
24	Rack mountable with rail/mount kit		
25	Must comply with recognized safety, EMC & environmental standards such as UL/IEC safety, FCC/ETSI EMC, and RoHS environmental compliance.		

6.3.14 SIEM Solution (Security Incident and Event Management Solution) (SL 17)

Sl No	Specification	Proposed Specification	Compliance (Yes/No)
1	The Solution should support Ingests logs and telemetry from servers/VMs, network and security equipment without endpoint agents.		
2	The Solution should support Performs parsing, normalization, correlation, detection, alerting, investigation, and reporting via a web UI.		
3	The Solution should support Linux collectors receiving Syslog (UDP/TCP/TLS), RELP(+TLS), HTTP/HTTPS, and Windows Event Forwarding (WEF) via a Windows Event Collector (WEC). Forward to the analytics tier using open- source pipelines.		
4	The Solution should support Stateless parsing/enrichment pipeline services (e.g., GROK/regex, JSON, KV, CEF/LEEF) applying routing, tagging, timestamp & timezone correction, geo/IP reputation, threat-intel enrichment (STIX/TAXII or file-based).		
5	The Solution should support Distributed, horizontally scalable, open-source search/analytics engine (REST/JSON DSL, time-series aggregations) with index lifecycle management (hot/warm/cold), snapshots to S3-compatible object storage, RBAC, audit logs, and fine- grained		
6	The Solution should support Open-source detection engine integrated with the analytics cluster, supporting rule authoring, Sigma rule import, scheduling, findings, correlation, alerting, and MITRE ATT&CK mapping.		
7	The Solution should support Web dashboards for search, timelines, alerts, cases, and reports; multi-tenant workspaces; API access.		
8	The Solution should support Flow telemetry collector for NetFlow/IPFIX/sFlow feeding the analytics cluster.		
9	The Solution should support Syslog (RFC3164/5424) over UDP/TCP, Syslog-TLS (6514), RELP(+TLS), HTTP/HTTPS, WEF/WEC for Windows Events.		
10	The Solution should support Must sustain the committed peak EPS with back-pressure and buffering; lossless delivery over reliable transports (RELP/HTTPS).		
11	The Solution should support Pluggable pipelines for parse, enrich, route with field mappings to a normalized schema		
12	The Solution should support Built-in/packaged parsers for common network/security devices; tooling to create/extend parsers without code.		
13	The Solution should supportSTIX/TAXII 2.x client or file-feed ingestion (hashes, IPs, domains, URLs).		
14	The Solution should support On-ingest or on-query enrichment (GeoIP, ASN, private lookup tables).		
15	The Solution should support Configurable TTL and versioning for TI feeds.		
16	The Solution should support Distributed cluster with dedicated node roles		
17	The Solution should support RESTful API & JSON DSL with boolean queries, aggregations, windowed time-series (date_histogram), and saved searches.		

18	The Solution should support threshold, sequence/correlation across indices, anomaly by aggregation baselines, and schedule-based queries.		
19	The Solution should support native import/export of Sigma rules; rule tagging and mapping to MITRE ATT&CK TTPs.		
20	The Solution should support de-duplication, suppression windows, severity, labels, owners, and routing to email/SMTP, webhook, chat, or ITSM.		
21	The Solution should support Provide a starter library (≥300 rules) covering auth, privilege abuse, lateral movement, network scanning, malware indicators, data exfiltration, and cloud/virtualization logs (generic).		
22	The Solution should support per-rule index filters, exceptions/lists, lookup tables, and environment variables (e.g., critical assets, service accounts).		
23	The Solution should support Prebuilt dashboards for auth, endpoint (syslog), network/security devices, and infrastructure.		
24	The Solution should support Timeline view for multi-event investigations; pivoting from alerts to raw events.		
25	The Solution should support Case management: built-in OR integrate via REST/webhooks to an open-source case system; support tasks, comments, attachments, assignees, status, SLA clocks, and audit trail.		
26	The Solution should support Reporting, scheduled PDF/CSV exports; role-scoped scheduled delivery.		

6.3.15 Monitoring Tool (SL 18)

Sl No	Specification	Proposed Specification	Compliance (Yes/ No)
1	Data Collection: Support agent-based and agentless collection (SNMP, IPMI, APIs, custom scripts/exporters).		
2	Flexible Scheduling: Configurable polling intervals with support for frequent or throttled data collection.		
3	Metric Types: Handle counters, gauges, logs, structured formats (JSON, XML, etc.).		
4	Alerting: Thresholds, anomaly detection, escalation policies, multi-channel notifications.		
5	Dashboards & Visualization: Customizable UI with charts, service maps, drill-down and scheduled reports.		
6	Scalability & Architecture: Distributed or clustered deployment, high availability, horizontal scaling.		
7	Historical Data Retention: Configurable retention and long-term archival with compression.		
8	Auto-Discovery: Discover hosts, services, VMs/containers automatically with network/cloud scans.		
9	Integration: APIs and plugins for cloud, virtualization, ticketing, ChatOps (Slack, Jira, etc.).		
10	Security: RBAC, LDAP/SAML, TLS encryption, audit logs.		
11	Configuration Management: Template-based setup, automation tools (Ansible, CLI, API), version control.		
12	Licensing & Community: Open-source license, active community, documentation and support.		

6.3.16 KVM with KMM Switch (Type-1 and Type-2) (SL 19 and SL 20)

SL	Minimum Specifications	Proposed Specification	Compliance (Yes/ No)
1.	Make		
2.	Model		
3.	Integrated 17" LCD KVM console in slide-out/slideaway housing		
4.	LCD console with adjustable viewing angle and comp switches	atibility with USB	-based KVM
5.	Minimum 16 USB ports		
6.	Built-in internal or external power supply		
7.	Adjustable rack depth compatibility		
8.	Supports video resolution up to 1280× 1024 @ 75Hz		
9.	Should be rack-mountable in standard equipment racks		

6.3.17 Security Operations Centre (SL 21)

SL	Technical Requirement	Proposed Specification	Compliance (Yes/No)
1	**SOC Architecture:** SOC may be open-source solutions without vendor lock-in.		
2	**SIEM Platform:** Should support open-source SIEM or property SIEM with log ingestion, correlation, dashboards, and alerting. Must support horizontal scaling.		
3	**Log Collection:** Support agent-based and agentless collection (Syslog, Beats, API, custom scripts). Must integrate with servers, firewalls, proxies, endpoints, cloud, databases.		
4	**Log Retention:** Minimum 365 days online + 5 years archival using open technologies		
5	**SOAR Capabilities:** Integration with open-source SOAR with automated playbooks, enrichment, and ticketing workflows.		
6	**Threat Intelligence:** Must support MISP or any STIX/TAXII-based open-intel platform. Should correlate TI indicators with SIEM events.		
7	**UEBA Capabilities:** Should support anomaly detection using machine learning.		

8	**Network Detection:** Must support integration with open-source NDR tools for deep packet inspection, traffic analysis, and behavioral detection.		
9	**Endpoint Detection:** Should support open-source EDR (Wazuh agents) with process monitoring, file integrity, malware detection, and auto-isolation capability.		
10	**Vulnerability Assessment:**		
	Must integrate with open-source VA tools like OpenVAS/Greenbone. Automated scanning, CVSS scoring, prioritization.		
11	**Cloud Monitoring:** Support cloud logs via API		
12	**Correlation Rules:** Support custom rules in Sigma format or equivalent open formats.		
13	**Dashboards & Visualization:** Fully customizable dashboards using Kibana/Grafana/Security Onion interface, with drill-down capability.		
14	**Incident Response:** Should provide incident case management via TheHive or similar open-source platform with escalation workflows.		
15	**Alerting :** Multi-channel alerts (Email, SMS Gateway, Webhooks, Slack, MS Teams, Telegram, etc.).		
16	**Compliance Standards:** Must support compliance mappings (ISO 27001, NIST 800- 53, CERT-In guidelines, CIS benchmarks).		
17	**Auto-Discovery:** System should detect servers, network devices, VMs/containers automatically using open-source discovery mechanisms.		
18	**API Support:** RESTful APIs for integration with other tools, ITSM, automation layers.		
19	**RBAC:** Role Based Access Control with granular privileges for SOC		
20	**Authentication:** LDAP/AD/SAML/OAuth2 integration for identity-based access.		
21	**Encryption:** TLS 1.2+ for data in transit; disk encryption options for data at rest (LUKS, dm-crypt, etc.).		

22	**Reporting:** Daily/Weekly/Monthly reports with automated schedules (PDF/CSV/HTML) via open-source tools.		
23	**24x7 Monitoring:** Solution must support continuous monitoring setup with centralized console and distributed agents/sensors.		
24	**High Availability:** All core components must support clustering and failover using open-source mechanisms.		
25	**Scalability:** Must scale horizontally by adding nodes with no vendor licensing constraints.		
26	**Backup & Archival:** Support S3-compatible object storage, NAS, or open- source backup tools (Restic, Bacula).		
27	**Security Standards:** Must follow secure hardening guidelines for all components		
28	**Training:** Bidder must provide training and knowledge transfer on all deployed open-source tools.		

29	**Documentation:** Detailed design documents, runbooks, SOPs, and playbooks must be provided.		
30	**Source Code Integrity:** All custom scripts/playbooks must be open, auditable, and provided to the department.		
31	**Zero Vendor Lock-In:** Should not require proprietary tools, licenses, or locked appliances		
32	**Governance :** SOC dashboards for leadership, SLA tracking, incident KPIs.		
33	**SLA Requirements**: Defined response times for alerts (Critical: 15 mins, High: 30 mins), SOC uptime 99.9%.		

6.3.18 Venerability assessment tools (SL 22)

SL	Minimum Specification	Proposed Specification	Compliance (Yes/No)
1	The solution shall support comprehensive vulnerability scanning for servers, endpoints, network devices, security appliances, applications, and cloud workloads.		
2	Must support both authenticated and unauthenticated scans for OS, network, and web applications.		
3	The tool shall include regularly updated vulnerability feeds covering CVE, CWE, CVSS, OWASP Top 10, and emerging threats.		
4	Shall provide support for multiple scanning techniques: network scanning, port scanning, service enumeration, OS fingerprinting, and web application scanning.		
5	Must support configuration and compliance checks against industry standards such as CIS Benchmarks, STIGs, and best practices.		
6	Should support API-based integration for automation pipelines (CI/CD), ticketing systems, SIEM/SOC platforms, and dashboards.		
7	The solution shall generate detailed reports including risk categorization, severity scoring (CVSS v3.x), remediation guidance, and asset-wise vulnerability summaries.		
8	Must support customizable dashboards and scheduled reporting in formats such as PDF, CSV, JSON.		
9	Shall support discovery of network assets using passive and active scanning mechanisms.		
10	The tool should support container and container-orchestration vulnerability assessment (Docker, Kubernetes).		
11	Must support scanning of web applications for OWASP Top 10 vulnerabilities, including SQLi, XSS, CSRF, insecure configurations, and authentication flaws.		
12	Should support plugin-based extensible architecture allowing users to add custom scripts or rules.		
13	Shall support role-based access control (RBAC) and audit logging.		
14	Should support on-prem deployment without mandatory cloud dependency.		
15	Tool must support high-level scalability to handle large enterprise environments through distributed or agent-based scanning.		
16	Must provide secure communication channels (TLS/SSL) between console and scanning nodes.		
17	The solution should be platform-independent (Linux preferred, Windows compatible optional).		
18	Should provide false-positive management, vulnerability suppression, and verification scans.		
19	The tool must allow export/import of scan templates, policies, and rules.		
20	Compliance with security standards such as ISO 27001, NIST 800-53, and CERT advisories.		
21	The VA tool must support vulnerability and configuration assessment for S3-compatible object storage systems.		
22	The tool must detect publicly accessible buckets, objects, and URLs.		
23	The tool must analyze S3 ACLs, bucket policies, IAM permissions, and identify overly permissive configurations.		
24	The tool must assess encryption settings (SSE-S3, SSE- KMS, client-side encryption).		

25	The tool must verify object versioning, lifecycle policies, retention, and Object Lock settings.		
26	The tool must identify buckets without access logging, audit logging, or insufficient retention.		
27	The tool must scan S3 endpoints for TLS misconfiguration, insecure protocols, and outdated cipher suites.		
28	The tool must detect anonymous access, pre-signed URL exposure, and insecure upload/download endpoints.		
29	The tool must support discovery and assessment of S3 buckets across all storage zones/clusters.		
30	The tool must support API-based and automated scanning of S3-compatible object storage.		
31	Scanning engine should be scalable to scan minimum 10,000+ IPs without performance degradation.		

6.3.19 API monitoring solution (SL 23)

Sl. No	Minimum Specification	Proposed Specification	Compliance (Yes/No)
1	General Requirements: The API monitoring solution shall be open source with an active community and regular security updates. The solution shall be deployable on-premises or in a Government-approved cloud/data centre.		
4	API Availability Monitoring The tool shall support monitoring of HTTP/HTTPS REST APIs. Periodic health checks for API endpoints with configurable intervals.		
7	Performance Monitoring Monitor API response time, latency, and throughput. Support percentile metrics (Average, P95, P99 response times).		
	Track HTTP response codes (2xx, 4xx, 5xx) and error rates.		
10	SLA Monitoring Allow configuration of SLA/SLO thresholds per API. Generate SLA compliance reports (daily/monthly).		
12	Alerting & Escalation Provide rule-based alerting for downtime, latency, and error thresholds. Support alert notifications via email, SMS (gateway integration), and webhooks.		
15	Security Monitoring Support secure communication using TLS/HTTPS.		
20	Logging & Tracing Support log correlation and distributed tracing (e.g., OpenTelemetry/SkyWalking).		

21	Dashboard & Reporting Provide a web-based dashboard for real-time API monitoring.		
23	Integration & Extensibility Provide REST APIs for integration with ITSM, SIEM, and monitoring tools. Support integration with open-source API gateways (Apache APISIX, Tyk, Kong– OSS).		
25	User Management Support role-based access control (RBAC). Support integration with centralized IAM/LDAP/SSO (desirable).		
27	Audit & Compliance Maintain audit logs for user actions and configuration changes.		
28	Compliance & Security Comply with Government of India IT policies and CERT- In guidelines. Ensure monitoring data remains within Government-controlled infrastructure.		
30	Documentation & Support Provide complete technical documentation and community support.		

6.3.20 Clientless SSL VPN (SL 24)

Sl. No	Technical Specification	Proposed Specification	Compliance (Yes/No)
1	Clientless SSL VPN: Must provide secure browser-based access to internal applications without requiring client software installation.		
2	HTTPS/TLS Security: All sessions must use TLS 1.2 or TLS 1.3. Support strong ciphers, HSTS, and disable weak protocols (TLS 1.0/1.1).		
3	Application Access: Must allow granular access to web applications (HTTPS), internal portals, and web services via the browser.		
4	Authentication:		
	Must have MFA, LDAP, SSO, SAML, or OAuth2 for user authentication. Optionally support client certificates.		
5	Session Management: Must provide session timeouts, idle session termination, session logging, and protection against session hijacking.		
6	Policy & Role-Based Access: Must allow defining access policies per user/group, per application, per URL/path.		
7	High Availability:		

	Must have active-active or active-passive HA deployment to ensure continuous access.		
8	The SSL VPN solution shall provide clientless, browser- based remote desktop access to internal Windows and Linux servers without requiring any client software installation.		
9	The solution must support RDP, SSH over HTTPS with granular role-based access control.		
10	Monitoring & Logging: Must log all user sessions, failed login attempts, and provide alerts for suspicious activities. Integration with SIEM/SOC is optional.		
11	Performance & Scalability : Must have minimum concurrent sessions as required, with load balancing support for high availability.		
12	Compliance: Must comply with industry standards for web security (ISO 27001, OWASP Top 10, NIST guidelines).		

6.3.21 Windows Server Remote Desktop Environment for 150 users (SL 25)

Sl. No.	Technical Specification	Proposed Specification	Compliance (Yes/No)
1	User Access: The solution shall provide **150 concurrent Remote Desktop (RDP) connections** to a single Windows Server instance.		
2	Purpose: The environment shall enable developers/technical personal to install tools for development of application, and **create, edit, and store source code and application-related files** securely on the server.		
3	File Upload: Developers/ technical personal shall be able to **upload files from their local workstation to the server** for development purposes.		
4	File Download Restriction: The solution must **restrict downloading or copying of files from the server to local desktops** to ensure code and data security.		
5	Security & Compliance: The solution shall implement **role-based access control (RBAC)**, and secure authentication mechanisms to prevent unauthorized access.		
6	Scalability & Performance: The server must **support 150 concurrent users** without performance degradation and allow future scaling if required.		

7	Backup & Storage: The solution shall provide **centralized storage for source code and application files**, with regular backups and redundancy.		
8	Licensing Appropriate **Windows Server licenses and Remote Desktop Services (RDS) CALs for 150 users** shall be included as part of the solution.		

6.3.22 Cryptographic Security, Key Management & HSM Framework (Type-1 & Type-2) (SL 26 & SL 27)

SL	Specification / Requirement	Proposed Specification	Compliance (Yes/No)
1	**Scope :** Supply, installation, configuration, and support of Hardware Security Modules (HSMs) at both Data Centre (DC) and Disaster Recovery (DR) sites		
2	Deployment: Dedicated hardware HSM appliances to be deployed at DC and DR with high availability and disaster recovery capability		
3	Standards Compliance : HSMs shall be FIPS 140-3 Level 3 (or higher) compliant		
4	Regulatory Alignment : Solution shall comply with NIST, CERT-In, and applicable Government of India security guidelines		
5	Cryptographic Algorithms : Support AES-256, RSA, ECC, SHA-2 family, TLS 1.3, and IPSec		
6	Post-Quantum Readiness : Support hybrid (classical + PQC) cryptographic mechanisms aligned with NIST PQC standards		
7	Key Management : Secure key generation, storage, rotation, revocation, and deletion through centralized Key Management Services (KMS)		
8	Key Protection : Encryption keys shall be non-exportable in plain text form		
9	Key Isolation : Support tenant / department / project- level key isolation		
10	Access Control : Enforce Role-Based Access Control (RBAC) for key and HSM administration		
11	DC–DR Replication : Secure and automatic replication of cryptographic keys between DC and DR		
12	Disaster Recovery : DR site shall be immediately operational with replicated keys in case of DC failure		
13	High Availability : Support HSM clustering or redundancy for fault tolerance		
14	Workload Coverage : Support encryption for compute, storage, network, backup, and container workloads		
15	Compute Integration : Integration with physical servers and virtual machines		
16	Storage Integration : Integration with block, file, and object storage systems		
17	Network Security : Support TLS/IPSec for secure data- in-transit encryption		
18	Backup Security : Encryption support for backups and archival data at DC and DR		
19	Container Support : Integration with container platforms and orchestration systems		
20	Interfaces & APIs : Support PKCS#11, KMIP, and RESTful APIs		

21	Automation : Enable automation through APIs and management portals		
22	Audit Logging : All key management and cryptographic operations shall be logged		
23	Audit Compliance : Logs shall be tamper-proof and retained as per policy		
24	Monitoring : Provide health, performance, and security monitoring with alerts		
25	Licensing : All required licenses and subscriptions to be included in scope for five years		
26	Commercials : No additional cost for DC–DR replication, audit logging, or API usage		
27	Support : OEM-backed support including firmware updates and security patches for five years		
28	Documentation : Provide configuration documents, SOPs, and audit reports		
29	Knowledge Transfer : Training and handover to department officials		
30	Deliverables : HSM devices at DC & DR, configured KMS, replication setup, and compliance documentation		

Section-2

2.1. The Bidder will prepare the bid in two parts – Technical Bid and Financial Bid should be submitted as hard copy in two separate envelop sealed and signed by authorized signatory of the bidder. Each envelop should strictly mention 'Technical Bid' or 'Financial Bid' along with 'Tender Number' and "Name & Address of the Bidder", accordingly.

a) Technical Bid:

Bidder must ensure that Technical Bid do not contain any Commercial items / prices. All documents to be submitted in Hard Copy duly signed by authorized signatory of the bidder.

The Bid should comprise of the following documents: -

i. Document fee & EMD Particulars.

ii. Signed copy of the Bid Document.

iii. The bidder must affix a Court Fee Stamp of Rs. 100/- in the place provided on the original Bid document.

iv. Manufacturer Authorization Form from OEM for this particular bid needs to be submitted.

v. Datasheet/Fact Sheets for the product quoted by the Bidder.

vi. Quality and Standard Certifications obtained by OEM and the product being offered.

vii. Complete Bill of Material with Make and Model to be type written.

b) Financial Bid- Financial bids to be submitted in hard copy in a separately envelop.

2.3 Other Conditions of bid submission:

i) AMTRON will not hold any risk and responsibility regulating non-visibility of the printed documents. No document should be handwritten other than signature.
ii) The Bidder shall bear all costs associated with the preparation and submission of its bid including cost of presentation for the purposes of clarification of the bid. AMTRON, will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the Tendering process.
iii) The Bids prepared by the Bidder and all correspondence and documents relating to the bids exchanged by the Bidder and AMTRON, shall be written in English language, provided that any printed literature furnished by the Bidder may be written in another language so long the same is accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern.
iv) It shall be deemed that the bidders have done careful study and examination of the Tender/ bid document and has fully understood the implications.
v) The response to the Tender/ bid should be full and complete in all respects. Failure to furnish the requisite information or submission of a proposal not substantially responsive to the Tender/ bid

document in every respect will be at the bidder's risk and may result in rejection of the proposal and forfeiture of the EMD.

vi) All materials submitted by the bidder become the property of Information Technology Department and may be returned at its sole discretion.

2.4. General Instructions for Proposal Submission:

a) Submission of Technical Bid-

i. The bidders should submit the hardcopies of the documents listed in Clause 2.1.

ii. Technical bid should include all documents mentioned in Section 2, Technical Bid. Please Note that Prices should not be indicated in the Technical Proposal but should only be indicated in the Financial Proposal failing which the bid submitted shall be summarily rejected.

iii. Please note that all the formats given has to be duly filled up submitted in the bid failing which the bid submitted shall be summarily rejected.

SECTION-3

3.1. General Conditions of the Contract:

i. Bidder must have sufficient arrangements with patent / copyright holders in respect of Technology / licenses etc. Bidder must have requisite authorizations and clearances from Govt./Statutory/Tax authorities that enable it to execute such a supply order in the state of Assam.

ii. The bidder once selected, must ensure that the equipment supplied is brand new, first hand and contains no previously used, recycled, or refurbished components and is consistently of the same brand, specification and capability as that of the quoted equipment.

iii. The license supplied must be guaranteed by the Supplier OEM Company as a 1st party for proper operations, performance and correction of any malfunction. The guarantee period will commence from the date of hand over of the equipment after carrying out successfully the tests prescribed by the AMTRON and shall remain in force till the completion of the period of 1 (one) year or any other period so specified in the supply order. The warranty provided by the Bidder/(s) who is/are awarded the supply order/(s) shall provide OEM warranty.

iv. AMTRON reserves to right of inspection for technical conformity & quality of the equipment quoted, the manufacturing process, warranty service, facilities, by sampling or in full and by factory acceptance or at point of delivery, at times and in the manner, it deems fit & necessary.

v. Bidder shall enclose along with in the Technical bid, descriptive technical Literature & Technical Data Sheet in hard copy on the equipment quoted viz. specifications, features etc. in the form of product brochures etc. In addition, as a part of the evaluation process, Bidders are required to submit company sealed samples of the all the equipment quoted and intended for supply along with the tender bid on the date of submission of the tender bid failing which his tender is liable to be cancelled. AMTRON shall not be liable for payment for any cost incurred by the bidder on this account. Testing of the equipment quoted and intended for supply, for fulfilment, at the minimum, the technical specifications & requirements mentioned in the detailed in this Tender Document, and overall product suitability, ergonomics, user friendliness, features, compatibilities, limitations etc. will be carried out.

vi. AMTRON reserves the right to settle matters in regard to the final quantity of equipment to be supplied during finalization of the supply order.

vii. C form will not be provided by the Purchaser.

viii. Road Permit shall not be provided by the Purchaser.

3.2 Packing:

The equipment shall be packed in suitable packing boxes with proper cushioning material to avoid transit damages and in a manner so as to avoid transit damages, if any, from being blamed on faulty/defective packing. The burden of proof in such an event shall lie on the Vendor.

3.3 Inspection:

AMTRON reserves to right of inspection for technical conformity & quality of the equipment quoted, the manufacturing process, warranty service, facilities, by sampling or in full and in factory or at point of delivery, at times and in the manner, it deems fit & necessary.

3.4 Proposed Timelines:

The time schedule for the Supply Order will be as follows:

Activity	Time in days
Issue of Purchase Order	T
Delivery & handover of approved equipment	T+60 days

3.5 Consideration for the supply order:

1. Prices quoted in the bid must be firm and final and shall not be subject to any upward modifications, on any account whatsoever. However, the Purchaser reserves the right to negotiate the prices quoted in the bid to effect downward modification.
2. The Commercial bid should clearly indicate the price to be charged without any qualifications whatsoever and should include all taxes, duties, fees, levies, works contract tax and other charges as may be applicable in relation to the activities proposed to be carried out.
3. The taxes will be applicable as per the current rate. In case of any change in the applicable rates, the bidder shall bill according to the then prevalent rate. However, should there be a change in the applicable taxes Purchaser reserves the right to negotiate with the Bidder.
4. Prices shall be quoted in Indian National Rupees (INR).
5. The prices will be FOR.
6. AMTRON reserves the right to distribute the order among other, qualified bidder in a ratio it deems fit.
7. All payments will be made on the following milestones:

3.6 Payment Schedule:

Sl. No.	Milestone	% of Payment
1	Completion of supply and testing	After receipt of Fund from end user

3.7 Warranty Service:

All the material supplied must be guaranteed by respective Manufacturers, as first party guarantee for proper operations, performance and correction of any malfunction. The warranty period will commence from the date of installation of the license.

The warranty must include, if not mentioned herein otherwise, but not limited to the following: -

a) Free-of-cost all services required during the entire warranty period that should result in complete restoration of the equipment to its fully functional status.

b) Must provide for free-of-cost complete replacement of the concerned module of the equipment, for any fault, malfunctioning or defect found in the period of 90 days from the date of handover to the end-user.

c) Provide for services of rectification & maintenance for the warranty period.

The Bidder/(s) who is/are awarded the supply order/(s) shall handover, along with the licenses, all the operational and maintenance manuals, Warranty and support information to the purchaser along with authentic ownership/ purchase documents/ licenses, warranty certificate wherever applicable.

During performance of the Contract, the Supplier shall offer to the Purchaser all new versions, releases, and updates of Standard Software, as well as related documentation and technical support services, within thirty (30) days of their availability from the Supplier to other clients of the Supplier.

During the Warranty Period, the Supplier will provide at no additional cost to the Purchaser all new versions, releases, and updates for all Standard Software that are used in the System, within thirty (30) days of their availability from the Supplier to other clients of the Supplier.

In cases where the new version, release, or update adversely affects System operation or performance, or requires extensive reworking of the System, the Supplier shall continue to support and maintain the version or release previously in operation for as long as necessary to allow introduction of the new version, release, or update.

3.7 Bid Validity Period:

Bids shall remain valid for 30 days after the date of opening of Technical Bids prescribed by the Purchaser. A bid valid for a shorter period may be rejected as non-responsive. The prices excluding the taxes, finalized after opening the tenders shall not increase throughout the period of implementation.

Extension of Period of Validity: In exceptional circumstances, the Purchaser may request the Bidder(s) for an extension of the period of validity. The request and the responses thereto shall be made in writing (or by fax). The bidder shall be at liberty to refuse the request. In such a circumstance, it will be construed that the bidder has withdrawn his bid and will not be entitled to claim or receive any penalty/damages/ interest/charges. However, he will be entitled to return of his bid documents submitted and refund of the EMD.

3.9 Bid Evaluation Criteria:

i. Evaluation of Technical Bid:

All evaluation process will be carried out by a Tender Evaluation Committee for evaluation of technical bids and the commercial bid, to be formed by the Purchaser for this purpose. The decision of the Tender committee shall be final, and no correspondence will be entertained outside the process of negotiation by the Committee. Evaluation of the bid documents will be as shown below:

At this stage, the technical bid will be opened and examined for genuineness of the bid, documents for compliance to the qualification requirements, compliance of specifications of the Batteries, submission of EMD, adequacy of documents, whether any computational errors have been made, whether the documents have been properly signed and the documents are prima facie in order and information as stated to be required in this tender has been submitted, correct fulfilment of all required formalities. Tender will be studied to examine if the bidder has at least the minimum capability evidenced by fulfilment of the minimum levels of criteria & conditions mentioned in the NIT and in this tender. At this stage decisions of outright disqualification will be taken. A bid determined not substantially responsive will be rejected and may not subsequently be made responsive by the Bidder by correction of the nonconformity.

ii. Evaluation of Commercial Bid:

a) Financial Bids will be opened in presence of all the bidders available during the time of opening of Financial Bid.

b) Purchase Order will be awarded to the **L1 Bidder item-wise**.

c) Purchase Order will be awarded depending upon availability of fund.

d) AMTRON may seek price negotiation/reverse auction if deems reasonable.

Performa -B

DECLARATION REGARDING ACCEPTANCE OF TERMS & CONDITIONS CONTAINED IN THE TENDER DOCUMENT

To,

The Managing Director,

Assam Electronics Development Corporation Ltd.,

Industrial Estate, Bamunimaidan, Guwahati-781021

Sir,

I have carefully gone through the Terms & Conditions contained in the Tender Document [No_____-]. I declare that all the provisions of this Tender Document contained in Section-1 to Section-3 are acceptable to my Company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours very truly,

Name: _____

Designation: _____

Company: _____

Address: _____

FORM-C

Profile of the Company/firm

1) Name of the Company:

2) Constitution: Private Limited. Company / Public Limited company / PSU Company/Firm

3) Registration No. & date of the company:

4) Tax PAN No & date:

5) GST Registration No. & date:

6) Registered Office Address with Tel. No, Fax No., email ID:

7) Contact Office Address with Tel. No, Fax No., email ID:

•

Signature of the bidder with seal

Tender No. AEDC/DC-DR/2026-27/01 Dtd. 13/03/2026

PART II - FINANCIAL BID.

Name of the & Address of Bidder:

SL	Description	Qty	Unit Price (INR) (b)	AMOUNT (INR) (p=a X b)	GST (q)	TOTAL (INR) (p + q)
1	Rack Server (type-1)	12				
2	Rack Server (type-2)	17				
2	Rack Server (type-3)	1				
2	Rack Server (type-4)	1				
2	Rack Server (type-5)	2				
3	Unified Storage (type-1)	1				
3	Object Storage (type-1)	1				
4	Unified Storage (type-2)	1				
4	Object Storage (type-2)	1				
5	SAN Switch (type-1)	2				
6	SAN Switch (type-2)	2				
7	Virtual Tape Library	1				
8	Web Application Firewall	2				
9	Other Software	1				
10	Out of Band Management Switch (Type-1)	1				
11	Out of Band Management Switch(Type-2)	2				
12	Core/Spine Switch (Type-1)	2				
13	Core/Spine Switch (Type-2)	2				
14	Server/Leaf Switch (Type-1)	2				
15	Server/Leaf Switch (Type-2)	2				
16	Next Generation Firewall	2				
17	Security Incident and event Management tools (SIEM)	1				
18	Monitoring System	1				
19	KVM with KMM Switch (Type-1)	1				
20	KVM with KMM Switch (Type-2)	1				
21	Security Operations Center (SOC)	1				
22	Venerability assessment tools	1				
23	API monitoring solution	1				
24	Clientless Web SSL VPN	1				
25	Windows Server Remote Desktop Environment for 150 user	1				
26	Cryptographic Security, Key Management & HSM Framework (Type-1)	2				
27	Cryptographic Security, Key Management & HSM Framework (Type-2)	2				

Date:

Place:

Signature:

Name:

Designation:

Seal: