**GOVERNMENT OF KERALA**
**POLICE DEPARTMENT**
Vazhuthacaud, Thiruvananthapuram - 695010
Ph: 0471-2722566 Fax: 0471- 2722566
e-mail: aig2phq.pol@kerala.gov.in
www.keralapolice.gov.in

**H9/168170/2026/PHQ** **Dated: 15/09/2026**

# e-Government Procurement (e-GP)
# NOTICE INVITING TENDER

The Director General of Police & State Police Chief, Kerala Police Department, Government of Kerala invites online bids through the e-Procurement portal from eligible, reputed, and experienced firms/agencies having proven expertise in enterprise cybersecurity, cyber range solutions, digital forensics, AI-driven threat analytics, malware analysis, threat intelligence, incident management and turnkey technology infrastructure projects for the **Establishment of Integrated Cyber Security Software and Simulation Platforms with Supporting Hardware Infrastructure at the Police Training College, Thiruvananthapuram,** under the ASUMP Scheme 2026–27.

| | |
|---|---|
| **Tender No. & Date** | **KPET/39/2026/PHQ Dated 15.09.2026** |
| **Description of Work** | **Establishment of Integrated Cyber Security Software and Simulation Platforms with Supporting Hardware Infrastructure at the Police Training College, Thiruvananthapuram** as per the specification. |

| | |
|---|---|
| **Locations** | **Police Training College, Thiruvananthapuram** |
| **Estimated Amount** | **Rs. 3.71 Crores** |
| **Tender Fees** | (through online mode only)<br>Rs. 28,750 /- [Rupees Twenty eight thousand seven hundred and fifty Only] (GST extra)<br>18% GST amount on tender fees mentioned above shall be paid to GST Department directly by the bidder. |
| **Earnest Money Deposit** | Rs. 3,71,000/- (Rupees Three lakh and seventy one thousand Only) (through online mode/Bank Guarantee) |
| **Specifications** | Attached in the Tender document. |
| **Date and Time of Publication of e Tender** | **15.09.2026, 05:00 PM** |
| **Last date and time for online Submission of e Tender** | **28.09.2026, 12.00 NOON** |
| **Date and time of opening of e-Tender** | **29.09.2026, 03.00 PM** |
| **Place of bid opening** | Police Headquarters, Vazhuthacaud, Thiruvananthapuram- 695010 |
| **Date of Technical Evaluation** | **Bidders should be ready to attend the Technical Evaluation on any day within 1 week after bid opening date on short notice.** |
| **Address of Tender Inviting Authority** | State Police Chief, Kerala,<br>Vazhuthacaud,<br>Thiruvananthapuram - 695010<br>Ph: 0471-2722566<br>Mobile No. 9497996998<br>Fax: 0471-2722566<br>e-mail: aig2phq.pol@kerala.gov.in<br>Website: www.keralapolice.gov.in |

| | |
|---|---|
| **Bid Validity** | (Total Number of Days up to which the rates are to be firm) **180 days** |

The scope of work includes the design, supply, installation, configuration, customization, integration, testing, training, commissioning and **five (5)** years of comprehensive support and maintenance for an integrated enterprise cyber capability infrastructure comprising Cyber Range Software, AI-Driven Threat Analytics Platform, Threat Intelligence Platform, Digital Forensics Solutions, Incident Management System, Cyber Security Solutions, enterprise servers, storage systems, networking, security appliances, and all associated hardware, software, and supporting infrastructure, in accordance with the Technical Specifications, Bill of Quantities (BoQ) and tender conditions.

**Scope of Work**

The project shall be established at the 2nd Floor, Police Training College, under the Scheme of ASUMP 2026–2027, and shall include complete end-to-end supply, licensing, installation, configuration, customization, integration, testing, User Acceptance Testing (UAT), commissioning, documentation, training, knowledge transfer, warranty and comprehensive technical support.

The scope shall cover the complete integrated Cyber Range and Cyber Security ecosystem, comprising the specified Cyber Range/SIEM-XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Incident/Case and Evidence Management, Digital Forensics, Cyber Security Training/Research, IT Operations Monitoring and Cyber Security/AI Workstations, including all necessary hardware, software, licences/subscriptions, APIs, connectors, accessories and implementation components required for the successful implementation, integration and operation of the complete solution.

The solution shall be modular, scalable, interoperable and technology-neutral. The bidder may propose Proprietary/Commercial, Customized Open-Source or Hybrid solutions, provided that all specified functional, technical, security, performance, scalability, integration and support requirements are fully met. Equivalent or superior technologies, products, platforms and frameworks providing comparable or better functionality and meeting the prescribed requirements shall be acceptable.

For Proprietary/Commercial, Open-Source and Hybrid solutions, the bidder shall be fully responsible for all required customization, configuration, integration, security hardening, development, licensing/subscriptions, maintenance, updates/upgrades and technical support,

as applicable, without any reduction in the mandatory scope or functionality.

For Open-Source or Hybrid solutions, the bidder shall additionally be responsible for all customization, integration, security hardening, development, maintenance, updates/upgrades and technical support necessary to deliver a complete, secure and fully functional enterprise solution. The use of Open-Source components shall not result in any reduction in the mandatory scope, functionality, security, performance, scalability, interoperability or support requirements.

Where Open-Source components are proposed, the bidder shall have demonstrated capability and relevant experience in their enterprise deployment, customization, integration, maintenance and support, and shall provide the necessary customer references and documentary evidence.

The bidder shall submit a component-wise and year-wise cost breakup, clearly separating one-time and recurring costs, including licences/subscriptions, support/AMC, updates/upgrades, threat-intelligence feeds, connectors, customization, training and other applicable costs for Year 1 to Year 5, together with the cumulative Total Cost of Ownership (TCO).

The bidder shall demonstrate relevant experience in implementation of comparable Cyber Security, Cyber Range or integrated security solutions and shall provide details and documentary evidence of successfully installed/commissioned customer references, including customer name, work order/contract reference, scope, value, commissioning status and contact/reference details. Where Open-Source technologies are proposed, relevant experience in their customization and integration shall also be demonstrated.

The bidder shall be responsible for the complete integrated solution as a single point of responsibility, irrespective of the combination of Commercial, Open-Source or Hybrid components proposed. The prime bidder shall remain fully responsible for the performance, integration, interoperability and support of all OEM products, software, Open-Source components, specialist technologies and implementation partners engaged for the project.

The bidder may engage appropriate OEMs and/or specialist implementation partners, subject to the eligibility, subcontracting and prior-approval provisions of the tender, wherever applicable. Such engagement shall not dilute or transfer the prime bidder's responsibility for the complete Scope of Work, deliverables, performance, integration, warranty, support or contractual obligations.

The Department may require technical demonstration/Proof of Concept (PoC) during technical evaluation and may verify the customer references and credentials submitted by the bidder. Where a demonstration/PoC is required, it shall be conducted in accordance with

the uniform evaluation methodology, requirements and criteria prescribed in the tender.

All components necessary to meet the specified functional, technical, security, performance, scalability and integration requirements shall be deemed to form part of the bidder's complete solution, irrespective of whether such components are individually identified in the BOQ, provided such components are essential for delivering the specified functionality of the complete integrated solution.

- **Integrated Technical Scope / BOQ**

| Sl. | Technical Item | Core Scope |
|---|---|---|
| 1 | Enterprise Cyber Range Simulation, Training & Integrated SIEM/XDR Platform | Cyber Range, virtualization, SIEM/XDR, SOC analytics, orchestration, training and integration |
| 2 | Enterprise AI/ML Threat Analytics, Security Analytics & Threat Hunting Platform | AI/ML analytics layer on Department-provided AI/GPU infrastructure |
| 3 | Enterprise Threat Intelligence Platform (TIP) | IOC/TTP intelligence, feeds, enrichment, standards and API integration |
| 4 | Enterprise Malware Sandbox Appliance | Dedicated malware analysis, detonation, behavioural analysis and intelligence integration |
| 5 | Incident, Case & Digital Evidence Management and Security Response Workflow | Incident/case lifecycle, evidence management, chain of custody and response workflows |
| 6 | Enterprise Digital Forensic Analysis & Investigation Software Suite | Computer, mobile, memory, network and multimedia forensics |
| 7 | Cyber Range Scenarios, Cyber Security Training, Research, Capacity Building & Advanced Analysis | Training, exercises, research tools, OSINT, analysis and knowledge transfer |
| 8 | Enterprise Application, Infrastructure & IT Operations Monitoring Dashboard Platform | APM, servers, databases, networks, storage, virtualization, cloud, endpoints and ITSM |
| 9 | Enterprise High-Performance Cyber Security Workstation with Integrated Command Console | SOC/Cyber Range operator workstation, dual displays, console and peripherals |

- **Detailed Technical Specifications**

### 2.1 Enterprise Cyber Range Simulation, Training & Integrated SIEM/XDR Platform

| Parameter | Minimum Technical Requirement |
|---|---|
| Platform | Enterprise Cyber Range supporting ILT, practical labs, CTF, Red/Blue/Purple Team, attack simulation, Incident Response, Malware Analysis, Digital Forensics, SOC training, Cyber Crisis/Tabletop exercises and competency assessments. |
| Capacity | Minimum 200 concurrent trainees, 20 instructors, 300+ VMs, 10+ concurrent labs and 100+ scenarios, with minimum 50% future scalability. |
| Virtualization | VMware vSphere / Hyper-V / Proxmox VE Enterprise / |

| Parameter | Minimum Technical Requirement |
|---|---|
| | KVM/OpenStack or equivalent with HA, clustering, live migration, templates, snapshots/rollback, monitoring and API integration. |
| Range Management | Centralized web-based orchestration supporting automated VM/network provisioning, isolated environments, lab/scenario deployment, cloning, snapshots, rollback, automated reset, team management and scoring. |
| SIEM/XDR | Enterprise SIEM/XDR using Wazuh with OpenSearch or equivalent, supporting minimum 250 monitored assets, centralized log/event collection, correlation, alerting, threat detection and security analytics. |
| Threat & SOC Analytics | IOC matching, MITRE ATT&CK mapping, UEBA, FIM, vulnerability detection, threat hunting, risk-based alerting, SOC dashboards, reporting, incident/case management and workflow automation. |
| Integration | AD/LDAP, firewalls, IDS/IPS, DNS/DHCP, Suricata, Zeek, MISP, Malware Sandbox, Threat Intelligence, AI/ML Threat Analytics, SAN/NAS, Video Wall, IFMS and other enterprise/security infrastructure through standard interfaces/APIs. |
| Security | RBAC, MFA, SSL/TLS, audit logging, centralized authentication, backup and recovery. |
| Solution Model & Pricing | Proprietary/Commercial, Open-Source or Hybrid. Proprietary and Open-Source options shall be separately priced, including implementation, licenses/subscriptions and 5-year TCO. |
| Training | Minimum 15 working days Administrator Training + 20 working days Instructor Training, including scenario/lab development and Red/Blue/Purple Team, CTF, SOC and Incident Response exercises. |
| Implementation | Complete installation, configuration, customization, integration, testing, performance validation, UAT, commissioning, documentation, SOPs and knowledge transfer. |
| Support | Minimum 5 years comprehensive support, including software/security updates, patches, scenario updates, technical assistance and capacity building. |

2.2 Enterprise AI/ML Threat Analytics, Security Analytics & Threat Hunting Platform

| Parameter | Minimum Technical Requirement |
|---|---|
| Platform | Enterprise AI/ML-based Threat Analytics and Security Monitoring Platform, deployed on Department-provided AI/GPU Compute Servers and on-premises Data Centre infrastructure. |
| Architecture | AI/ML analytics layer integrated with the Cyber Range and SIEM/XDR platform; shall not require procurement/deployment of a duplicate SIEM/XDR environment. |
| AI/ML Framework | TensorFlow, PyTorch, Scikit-learn, MLflow, JupyterLab or equivalent enterprise AI/ML frameworks/tools. |
| AI Security Analytics | AI-assisted threat detection, anomaly detection, UEBA, behavioural analytics, predictive threat analytics, threat hunting, malware analytics, IOC correlation, MITRE ATT&CK mapping and risk scoring. |
| Data Sources | Windows, Linux, AD, firewalls, IDS/IPS, DNS, Syslog, NetFlow/IPFIX, Zeek, Suricata, Sysmon, PCAP and Cyber Range exercises. |
| SIEM/XDR Integration | Full integration with Wazuh/OpenSearch or equivalent SIEM/XDR |

| Parameter | Minimum Technical Requirement |
|---|---|
| | for logs, alerts, IOCs, risk scores and AI-generated threat intelligence. |
| Malware & Threat Intelligence | Integration with Enterprise Malware Sandbox and Threat Intelligence Platform for behavioural analysis, IOC extraction, correlation and threat-intelligence enrichment. |
| Custom AI/ML Development | Development/customization of AI/ML security use cases, models, detection rules, correlation rules, dashboards, automated reports and threat-hunting workflows. |
| Deployment & APIs | Containerized deployment using Docker or equivalent with REST API/standard interfaces. |
| Security | RBAC, SSL/TLS encryption, audit logging, secure authentication, backup and recovery. |
| Hardware Scope | Department-provided AI/GPU Compute Infrastructure. AI/GPU server hardware is excluded from this BOQ item unless specifically stated otherwise. |
| Implementation & Training | Installation, configuration, customization, integration, testing, UAT, administrator/SOC analyst training, documentation, SOPs, architecture diagrams and knowledge transfer. |
| Support | Minimum 5 years comprehensive software support, including upgrades, security patches, remote/onsite technical assistance and AI/ML solution support. |

2.3 Enterprise Threat Intelligence Platform (TIP)

| Parameter | Minimum Technical Requirement |
|---|---|
| Platform & Intelligence | Enterprise web-based TIP supporting centralized aggregation, correlation and management of IOCs, TTPs, malware, phishing, ransomware, botnet and vulnerability intelligence, with automated ingestion, enrichment, reputation analysis, threat scoring and campaign tracking. |
| Standards & Integration | STIX/TAXII, OpenIOC, YARA, Sigma, MITRE ATT&CK, CVE/NVD and MISP or equivalent; API integration with Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Malware Sandbox, Suricata, Zeek, Firewalls, EDR/XDR and other security infrastructure. |
| Management, Licensing & Support | IOC search, threat hunting, dashboards, alerts, reporting, intelligence sharing, RBAC, SSL/TLS, audit logging and backup/recovery. Include software licenses, threat-intelligence feeds and connectors, installation, integration, UAT, documentation, training and 5-year comprehensive updates and technical support. |

2.4 Enterprise Malware Sandbox Appliance

| Parameter | Minimum Technical Requirement |
|---|---|
| Appliance & Malware Analysis | Dedicated Malware Sandbox Appliance with minimum 16 CPU cores, 64 GB RAM, 2 × 960 GB Enterprise SSD in RAID-1, minimum 4 TB analysis storage and redundant power supplies. Static, dynamic and behavioural analysis, detonation, exploit/ransomware/zero-day detection and AI-assisted threat classification. |
| Threat Analysis & Intelligence | Windows, Linux, Android and macOS-related files/workloads, executables, scripts, PDF/Office documents, archives, email attachments and web downloads; automated IOC extraction, malware reports, MITRE ATT&CK mapping, threat scoring and |

| | |
|---|---|
| | signature/detection-artifact generation. |
| Integration | SIEM/XDR, NGFW, Threat Intelligence Platform, AI/ML Threat Analytics, Cyber Range, Email Security Gateway, WAF and other security infrastructure, including automated sample submission and verdict/IOC exchange. |
| Management, Licensing & Support | Centralized web management, RBAC, SSL/TLS, audit logging and reporting. Include all hardware, software, licenses, subscriptions, threat-intelligence updates and accessories, installation, integration, testing/UAT, documentation, administrator training and 5-year comprehensive onsite OEM warranty, updates and technical support. |

2.5 Incident, Case & Digital Evidence Management and Security Response Workflow

| Parameter | Minimum Technical Requirement |
|---|---|
| Incident & Case Management | Centralized incident registration, categorization, prioritization, assignment, escalation, investigation, case notes, approvals and complete incident/case lifecycle tracking. |
| Security Response Workflow | Configurable workflows for alert triage, task assignment, escalation, SLA tracking, investigation, containment, remediation, recovery and incident closure. |
| Digital Evidence Management | Centralized registration and management of digital evidence, evidence inventory, evidence assignment, QR/barcode identification, secure evidence attachment/storage and forensic workflow tracking. |
| Evidence Integrity & Chain of Custody | MD5, SHA-256 or stronger hashing, evidence integrity validation, chain-of-custody tracking, version control and complete audit trail. |
| Integration | SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence Platform, Malware Sandbox, Digital Forensic Software/Mobile Forensic Tools, Cyber Range, AD/LDAP and SAN/NAS evidence storage. |
| Dashboard & Reporting | Real-time incident/case/evidence status, severity, response time, SLA compliance, trends, KPIs, evidence tracking, audit trails and management/executive/forensic reports. |
| Security & Access | RBAC, MFA, SSL/TLS, centralized authentication, audit logging, secure API access, backup and recovery. |
| Implementation & Support | Installation/deployment, configuration, customization, integration, testing/UAT, documentation, administrator/user training and 5-year comprehensive software updates, maintenance and technical support. |

2.6 Enterprise Digital Forensic Analysis & Investigation Software Suite

| Parameter | Minimum Technical Requirement |
|---|---|
| Forensic Analysis Capability | Computer, Mobile, Memory, Network and Multimedia Forensic Analysis, including file-system analysis, deleted-file recovery, registry, email/browser artefacts, timeline analysis, memory forensics, malware-related artefact analysis and forensic reporting. |
| Evidence Acquisition & Mobile Forensics | Logical, file-system and physical acquisition where technically supported; disk/image acquisition and compatibility with forensic imaging appliances and hardware write-blocking/acquisition kits; Android and iOS mobile forensic acquisition/analysis where supported. |
| Image & Video | Enhancement, deblurring, frame-level analysis, |

| Parameter | Minimum Technical Requirement |
|---|---|
| Forensics | authentication/integrity examination, object tracking, metadata extraction and relevant multimedia forensic analysis. |
| Evidence Formats & Platforms | Windows, Linux, macOS, Android and iOS; RAW/DD, E01/Ex01, AFF/AFF4, VMDK, VHD/VHDX or equivalent. |
| Evidence Integrity & Case Management | MD5, SHA-1, SHA-256 or stronger hashing, evidence verification, bookmarking/tagging, chain-of-custody, case management, investigation notes, audit trails and customizable forensic reports. |
| Enterprise Integration | SIEM/XDR, Incident & Case Management, Threat Intelligence Platform, Malware Sandbox, Cyber Range and SAN/NAS evidence storage through APIs, IOC/file exchange or equivalent. |
| Licensing, Security & Support | Appropriate multi-user/concurrent licensing, centralized license/user management and RBAC; all software/licenses, installation, configuration, integration, testing/UAT, training, documentation and 5-year comprehensive updates/upgrades/support. |

2.7 Cyber Range Scenarios, Cyber Security Training, Research, Capacity Building & Advanced Analysis

| Parameter | Minimum Technical Requirement |
|---|---|
| Cyber Range Scenarios & Exercises | Cyber Range simulations, Red Team, Blue Team, Purple Team, CTF, Tabletop, Cyber Crisis, SOC, Incident Response, Digital Forensics, Malware Analysis and Threat Hunting exercises. |
| Training & Capacity Building | Instructor-led and hands-on training covering Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Incident/Evidence Management, Digital/Mobile Forensics, Blockchain Investigation, servers, storage, virtualization, networks, firewall and associated ICT/security solutions. |
| Research & Analysis Tools | Cybersecurity research, OSINT, threat research, data correlation, link/relationship analysis, timeline and graph analysis, visualization, dashboards and intelligence analysis, with AI/ML-assisted analytics where applicable. |
| Integration | Integration with Cyber Range, SIEM/XDR, Threat Intelligence, Digital Forensics, Incident & Evidence Management and other project platforms through APIs/interfaces. |
| Training Content & Knowledge Transfer | Training manuals, SOPs, administrator/user guides, laboratory exercises, scenarios, presentations, case studies, assessments and Train-the-Trainer (ToT), including refresher/advanced training during support period. |
| Implementation Model & Support | Training/scenarios and research tools shall be provided module-wise and as required by the Department; licensing, customization, configuration, updates and technical support shall be included. |

2.8 Enterprise Application, Infrastructure & IT Operations Monitoring Dashboard Platform

| Parameter | Minimum Technical Requirement |
|---|---|
| Platform | Enterprise web-based Application & Infrastructure Monitoring Dashboard Platform with centralized administration and management. |
| Monitoring Capability | Centralized monitoring of applications/APM, servers, databases, networks, storage, virtualization, cloud infrastructure and endpoints. |

| Parameter | Minimum Technical Requirement |
|---|---|
| Dashboard & Analytics | Real-time interactive dashboards, customizable widgets, KPI monitoring, reports, analytics, alerts, notifications, historical data and trend analysis. |
| Infrastructure Integration | Windows, Linux, VMware/Hyper-V, Docker/containers, databases, storage, network/security devices, SNMP, Syslog, WMI and REST APIs. |
| Enterprise Integration | AD/LDAP, Cyber Range, SIEM/XDR, SAN/NAS, servers, network infrastructure and departmental applications/platforms. |
| IT Operations & Automation | Workflow automation, asset inventory, configuration management, SLA monitoring, helpdesk/ticketing integration and ITSM capabilities. |
| Alerts & Reporting | Threshold/event alerts, scheduled reports, email/SMS or equivalent notifications, performance analysis and capacity/trend reporting. |
| Security | RBAC, centralized authentication, SSL/TLS encryption, audit logging and backup/restore. |
| Solution Model | Zoho/ManageEngine or equivalent enterprise platform meeting/exceeding the specified requirements. |
| Licensing | All required licenses/subscriptions, connectors, monitoring agents, APIs and management components. |
| Implementation | Supply, installation, configuration, customization, integration, testing, UAT and commissioning. |
| Documentation & Training | Architecture/configuration documentation, SOPs, administrator training, user training and knowledge transfer. |
| Support | Minimum 5 years comprehensive software support including updates, upgrades, security patches and technical assistance. |

## 2.9 Enterprise High-Performance Cyber Security Workstation with Integrated Command Console

| Sl. No. | Feature | Minimum Technical Requirement |
|---|---|---|
| 1 | Type | Enterprise high-performance AI-enabled workstation/desktop AI appliance with integrated ergonomic operator/command console, suitable for SOC, Cyber Range, Red/Blue/Purple Team, AI/ML Threat Analytics, malware analysis, digital forensics and advanced cyber-security operations. |
| 2 | Make/Model | Product make and model shall be specified by the bidder. OEM technical datasheet shall be submitted along with the bid. Equivalent or superior products meeting all mandatory requirements shall be acceptable. |
| 3 | Monitor | Minimum 24-inch FHD IPS display, height-adjustable, with minimum 1 × HDMI and 1 × USB Type-C port. |
| 4 | Architecture | Architecture optimized for AI workloads, with tightly integrated CPU-GPU communication, high-bandwidth memory architecture and AI-focused compute capability suitable for local AI inference, model development and cyber-security analytics. |
| 5 | AI Compute Performance | Minimum 1 PFLOP / 1000 TFLOPS FP4 AI compute performance, or equivalent/superior AI inferencing capability. |
| 6 | AI Model Capacity – Single Node | The workstation shall support deployment/inference of AI models of up to 200 billion parameters on a single system, subject to the supported model framework and software environment. |
| 7 | AI Model Capacity – Two Node | The proposed architecture shall support AI models of up to 400 billion parameters using a two-node configuration, with the required high-speed interconnect and OEM-supported interconnect cables/accessories. |

| Sl. No. | Feature | Minimum Technical Requirement |
|---|---|---|
| 8 | Processor | AI-optimized processor architecture with minimum 20 CPU cores and integrated CPU-GPU architecture. NVIDIA GB10 or equivalent/superior architecture may be proposed. |
| 9 | CPU Cache | Minimum 16 MB L2 cache, or equivalent/superior processor cache architecture. |
| 10 | System Memory | Minimum 128 GB unified/coherent system memory or equivalent high-bandwidth memory architecture suitable for AI workloads. |
| 11 | Memory Architecture | Preference shall be given to unified or coherent memory architecture rather than fragmented CPU and GPU memory pools, provided the proposed architecture meets or exceeds the specified AI performance and capacity requirements. |
| 12 | Storage | Minimum 1 TB NVMe local storage, PCIe Gen4 or better, with provision for additional storage where required. |
| 13 | GPU / AI Accelerator | Enterprise AI GPU/accelerator based on NVIDIA Blackwell architecture or equivalent/superior technology, capable of meeting or exceeding the specified AI compute and model-capacity requirements. |
| 14 | Operating System | Linux-based AI-optimized operating system suitable for AI/ML workloads, containerized workloads, cybersecurity tools and enterprise management. Support for required virtualization/container technologies shall be provided. |
| 15 | Networking – Ethernet | Minimum 10GbE RJ-45 connectivity. |
| 16 | High-Speed Interconnect | Minimum 2 × QSFP high-speed ports, supporting aggregate/interconnect bandwidth of 200 Gbps or higher, or equivalent/superior high-speed node-to-node interconnect technology required for multi-node AI workloads. |
| 17 | Wireless Connectivity | Minimum Wi-Fi 6E or better and Bluetooth 5.4 or better, with integrated/internal antenna where applicable. |
| 18 | USB / I/O Ports | Minimum: 1 × USB 3.2 Gen 2x2 (20 Gbps) Type-C port with DisplayPort Alt Mode and power input; 3 × USB 3.2 Gen 2x2 (20 Gbps) Type-C ports with DisplayPort Alt Mode; and 1 × HDMI 2.1 or better port, or equivalent/superior I/O configuration. |
| 19 | Display Support | Shall support multiple high-resolution external displays suitable for SOC/Cyber Range operations and AI/cyber-security workflows. |
| 20 | Security | Minimum TPM 2.0, Secure Boot, hardware/firmware security controls, BIOS/UEFI security and storage encryption capability. |
| 21 | AI/ML Software Compatibility | Shall support enterprise AI/ML frameworks and tools including TensorFlow, PyTorch, Scikit-learn, MLflow, JupyterLab or equivalent, together with required GPU acceleration, containerization and development environments. |
| 22 | Cyber Security Software Compatibility | Shall support installation and operation of required Cyber Range, SIEM/XDR, SOC monitoring, packet/network analysis, Threat Intelligence, Malware Analysis, Digital Forensics, AI/ML Threat Analytics and security-analysis tools, subject to the respective software's platform requirements. |
| 23 | Integration | Shall support integration with Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Digital Forensics platforms, AD/LDAP, centralized authentication, network/security infrastructure and other approved enterprise systems through standard interfaces/APIs wherever applicable. |
| 24 | Virtualization / Containers | Shall support required virtualization and container technologies for deployment of approved Cyber Security, AI/ML and Cyber Range workloads, subject to the capabilities of the proposed platform. |
| 25 | Management | Enterprise-grade system monitoring, firmware/driver management, hardware health monitoring and centralized management capability shall be supported. |
| 26 | Command Console | Professional ergonomic operator/command console with dual/multi-monitor mounting provision, concealed cable management, power/data provisions and suitable equipment/storage space. |
| 27 | Seating | Heavy-duty, high-back ergonomic operator chair with adjustable height, lumbar support and adjustable armrests. |
| 28 | Peripherals | Professional keyboard and mouse, USB headset with microphone, Full-HD or better webcam, required power cables, display cables, adapters and all accessories necessary for complete operation. |
| 29 | AI Factory / Data- | Preference may be given to an OEM ecosystem capable of providing both the desktop |

| Sl. No. | Feature | Minimum Technical Requirement |
|---|---|---|
| | Centre Alignment | AI appliance/workstation and corresponding data-centre/server-scale AI infrastructure, enabling seamless transition from workstation-scale AI development/inference to server/cluster-scale deployment. This shall not restrict equivalent or superior solutions meeting the mandatory requirements. |
| 30 | Installation & Integration | Complete supply, installation, configuration, customization, integration, testing, performance validation, UAT and commissioning, including required drivers, firmware, software environment and approved security configuration. |
| 31 | Documentation | OEM technical datasheet, architecture documentation, configuration documentation, user/administrator manuals and relevant operational documentation shall be provided. |
| 32 | Warranty & Support | Minimum 5-year comprehensive onsite OEM warranty and technical support, including hardware defect rectification/replacement, applicable firmware/driver updates, technical assistance and support for the supplied platform. |
| 33 | High-Speed Interconnect Accessories | All OEM-recommended cables, QSFP modules, adapters, transceivers and accessories required for the specified two-node AI configuration shall be included. |
| 34 | Completeness | All hardware, software, licences, drivers, firmware, accessories, interconnects and implementation components necessary to achieve the specified functionality and performance shall be included in the bidder's complete solution. |

- **Technical Compliance Statement & Status**

The bidder shall submit a line-by-line compliance statement against every requirement. The bidder shall not merely state 'Complied'; supporting document reference, page number, model/part number, license type and deviation (if any) shall be stated wherever applicable.

Recommended status values: COMPLIED / PARTIALLY COMPLIED / NOT COMPLIED / DEVIATION / NOT APPLICABLE. Any deviation from a minimum requirement shall be explicitly declared. Silence or blank status may be treated as non-compliance at technical evaluation.

| Sl. No | Specification / Requirement | Bidder Compliance Status | Offered Specification / Model | Deviation / Remarks | Supporting Document / Page |
|---|---|---|---|---|---|
| 1 | Enterprise Cyber Range – capacity, virtualization, orchestration, SIEM/XDR and training requirements | | | | |
| 2 | AI/ML Threat Analytics – framework, analytics, telemetry, SIEM/XDR integration and custom AI/ML | | | | |
| 3 | Threat Intelligence Platform – standards, feeds, enrichment, integration and support | | | | |
| 4 | Enterprise Malware Sandbox Appliance – appliance hardware, analysis, integration and 5-year support | | | | |
| 5 | Incident, Case & Digital Evidence Management – lifecycle, evidence, chain of custody and workflow | | | | |
| 6 | Digital Forensic Analysis Suite – | | | | |

| Sl. No | Specification / Requirement | Bidder Compliance Status | Offered Specification / Model | Deviation / Remarks | Supporting Document / Page |
|---|---|---|---|---|---|
| | computer/mobile/memory/network/multimedia forensics and evidence formats | | | | |
| 7 | Cyber Range Training, Research & Capacity Building – exercises, OSINT, research, ToT and knowledge transfer | | | | |
| 8 | Application/Infrastructure Monitoring Dashboard – APM, servers, databases, network, storage, cloud, endpoints and ITSM | | | | |
| 9 | High-Performance Cyber Security Workstation + Command Console – workstation, displays, console, peripherals and 5-year warranty | | | | |

- **Detailed Line-by-Line Compliance Matrix – Bidder Format**

For every parameter under Section 5, the bidder shall reproduce/complete the following matrix. This matrix is intended to become the Technical Bid compliance statement.

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| 1 | Platform | Enterprise Cyber Range supporting ILT, practical labs, CTF, Red/Blue/Purple Team, attack simulation, Incident Response, Malware Analysis, Digital Forensics, SOC training, Cyber Crisis/Tabletop exercises and competency assessments. | | | |
| 1.1 | Capacity | Minimum 200 concurrent trainees, 20 instructors, 300+ VMs, 10+ concurrent labs and 100+ scenarios, with minimum 50% future scalability. | | | |
| 1.2 | Virtualization | VMware vSphere / Hyper-V / Proxmox VE Enterprise / KVM/OpenStack or equivalent with HA, clustering, live migration, templates, snapshots/rollback, | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | monitoring and API integration. | | | |
| 1.3 | Range Management | Centralized web-based orchestration supporting automated VM/network provisioning, isolated environments, lab/scenario deployment, cloning, snapshots, rollback, automated reset, team management and scoring. | | | |
| 1.4 | SIEM/XDR | Enterprise SIEM/XDR using Wazuh with OpenSearch or equivalent, supporting minimum 250 monitored assets, centralized log/event collection, correlation, alerting, threat detection and security analytics. | | | |
| 1.5 | Threat & SOC Analytics | IOC matching, MITRE ATT&CK mapping, UEBA, FIM, vulnerability detection, threat hunting, risk-based alerting, SOC dashboards, reporting, incident/case management and workflow automation. | | | |
| 1.6 | Integration | AD/LDAP, firewalls, IDS/IPS, DNS/DHCP, Suricata, Zeek, MISP, Malware Sandbox, Threat Intelligence, AI/ML Threat Analytics, SAN/NAS, Video Wall, IFMS and other enterprise/security infrastructure through standard interfaces/APIs. | | | |
| 1.7 | Security | RBAC, MFA, SSL/TLS, audit logging, centralized authentication, backup and recovery. | | | |
| 1.8 | Solution Model & Pricing | Proprietary/Commercial, Open-Source or Hybrid. Proprietary and Open-Source options shall be | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | separately priced, including implementation, licenses/subscriptions and 5-year TCO. | | | |
| 1.9 | Training | Minimum 15 working days Administrator Training + 20 working days Instructor Training, including scenario/lab development and Red/Blue/Purple Team, CTF, SOC and Incident Response exercises. | | | |
| 1.9 | Implementation | Complete installation, configuration, customization, integration, testing, performance validation, UAT, commissioning, documentation, SOPs and knowledge transfer. | | | |
| 1.10 | Support | Minimum 5 years comprehensive support, including software/security updates, patches, scenario updates, technical assistance and capacity building. | | | |
| 2 | Platform | Enterprise AI/ML-based Threat Analytics and Security Monitoring Platform, deployed on Department-provided AI/GPU Compute Servers and on-premises Data Centre infrastructure. | | | |
| 2.1 | Architecture | AI/ML analytics layer integrated with the Cyber Range and SIEM/XDR platform; shall not require procurement/deployment of a duplicate SIEM/XDR environment. | | | |
| 2.2 | AI/ML Framework | TensorFlow, PyTorch, Scikit-learn, MLflow, JupyterLab or equivalent enterprise AI/ML | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | frameworks/tools. | | | |
| 2.3 | AI Security Analytics | AI-assisted threat detection, anomaly detection, UEBA, behavioural analytics, predictive threat analytics, threat hunting, malware analytics, IOC correlation, MITRE ATT&CK mapping and risk scoring. | | | |
| 2.4 | Data Sources | Windows, Linux, AD, firewalls, IDS/IPS, DNS, Syslog, NetFlow/IPFIX, Zeek, Suricata, Sysmon, PCAP and Cyber Range exercises. | | | |
| 2.5 | SIEM/XDR Integration | Full integration with Wazuh/OpenSearch or equivalent SIEM/XDR for logs, alerts, IOCs, risk scores and AI-generated threat intelligence. | | | |
| 2.6 | Malware & Threat Intelligence | Integration with Enterprise Malware Sandbox and Threat Intelligence Platform for behavioural analysis, IOC extraction, correlation and threat-intelligence enrichment. | | | |
| 2.7 | Custom AI/ML Development | Development/ customization of AI/ML security use cases, models, detection rules, correlation rules, dashboards, automated reports and threat-hunting workflows. | | | |
| 2.8 | Deployment & APIs | Containerized deployment using Docker or equivalent with REST API/standard interfaces. | | | |
| 2.9 | Security | RBAC, SSL/TLS encryption, audit logging, secure authentication, backup and recovery. | | | |
| 2.9 | Hardware Scope | Department-provided AI/GPU Compute | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | Infrastructure. AI/GPU server hardware is excluded from this BOQ item unless specifically stated otherwise. | | | |
| 2.10 | Implementation & Training | Installation, configuration, customization, integration, testing, UAT, administrator/SOC analyst training, documentation, SOPs, architecture diagrams and knowledge transfer. | | | |
| 2.11 | Support | Minimum 5 years comprehensive software support, including upgrades, security patches, remote/onsite technical assistance and AI/ML solution support. | | | |
| 3 | Platform & Intelligence | Enterprise web-based TIP supporting centralized aggregation, correlation and management of IOCs, TTPs, malware, phishing, ransomware, botnet and vulnerability intelligence, with automated ingestion, enrichment, reputation analysis, threat scoring and campaign tracking. | | | |
| 3.1 | Standards & Integration | STIX/TAXII, OpenIOC, YARA, Sigma, MITRE ATT&CK, CVE/NVD and MISP or equivalent; API integration with Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Malware Sandbox, Suricata, Zeek, Firewalls, EDR/XDR and other security infrastructure. | | | |
| 3.2 | Management, Licensing & Support | IOC search, threat hunting, dashboards, alerts, reporting, intelligence sharing, RBAC, SSL/TLS, | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | audit logging and backup/recovery. Include software licenses, threat-intelligence feeds and connectors, installation, integration, UAT, documentation, training and 5-year comprehensive updates and technical support. | | | |
| 4 | Appliance & Malware Analysis | Dedicated Malware Sandbox Appliance with minimum 16 CPU cores, 64 GB RAM, 2 × 960 GB Enterprise SSD in RAID-1, minimum 4 TB analysis storage and redundant power supplies. Static, dynamic and behavioural analysis, detonation, exploit/ransomware/zero-day detection and AI-assisted threat classification. | | | |
| 4.1 | Threat Analysis & Intelligence | Windows, Linux, Android and macOS-related files/workloads, executables, scripts, PDF/Office documents, archives, email attachments and web downloads; automated IOC extraction, malware reports, MITRE ATT&CK mapping, threat scoring and signature/detection-artifact generation. | | | |
| 4.2 | Integration | SIEM/XDR, NGFW, Threat Intelligence Platform, AI/ML Threat Analytics, Cyber Range, Email Security Gateway, WAF and other security infrastructure, including automated sample submission and verdict/IOC | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | exchange. | | | |
| 4.3 | Management, Licensing & Support | Centralized web management, RBAC, SSL/TLS, audit logging and reporting. Include all hardware, software, licenses, subscriptions, threat-intelligence updates and accessories, installation, integration, testing/UAT, documentation, administrator training and 5-year comprehensive onsite OEM warranty, updates and technical support. | | | |
| 5 | Incident & Case Management | Centralized incident registration, categorization, prioritization, assignment, escalation, investigation, case notes, approvals and complete incident/case lifecycle tracking. | | | |
| 5.1 | Security Response Workflow | Configurable workflows for alert triage, task assignment, escalation, SLA tracking, investigation, containment, remediation, recovery and incident closure. | | | |
| 5.2 | Digital Evidence Management | Centralized registration and management of digital evidence, evidence inventory, evidence assignment, QR/barcode identification, secure evidence attachment/storage and forensic workflow tracking. | | | |
| 5.3 | Evidence Integrity & Chain of Custody | MD5, SHA-256 or stronger hashing, evidence integrity validation, chain-of-custody tracking, version control and complete audit trail. | | | |
| 5.5 | Integration | SIEM/XDR, AI/ML Threat | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | Analytics, Threat Intelligence Platform, Malware Sandbox, Digital Forensic Software/Mobile Forensic Tools, Cyber Range, AD/LDAP and SAN/NAS evidence storage. | | | |
| 5.6 | Dashboard & Reporting | Real-time incident/case/evidence status, severity, response time, SLA compliance, trends, KPIs, evidence tracking, audit trails and management/executive/forensic reports. | | | |
| 5.7 | Security & Access | RBAC, MFA, SSL/TLS, centralized authentication, audit logging, secure API access, backup and recovery. | | | |
| 5.8 | Implementation & Support | Installation/deployment, configuration, customization, integration, testing/UAT, documentation, administrator/user training and 5-year comprehensive software updates, maintenance and technical support. | | | |
| 6 | Forensic Analysis Capability | Computer, Mobile, Memory, Network and Multimedia Forensic Analysis, including file-system analysis, deleted-file recovery, registry, email/browser artefacts, timeline analysis, memory forensics, malware-related artefact analysis and forensic reporting. | | | |
| 6.1 | Evidence Acquisition & Mobile Forensics | Logical, file-system and physical acquisition where technically supported; disk/image acquisition and compatibility with forensic | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | imaging appliances and hardware write-blocking/acquisition kits; Android and iOS mobile forensic acquisition/analysis where supported. | | | |
| 6.2 | Image & Video Forensics | Enhancement, deblurring, frame-level analysis, authentication/integrity examination, object tracking, metadata extraction and relevant multimedia forensic analysis. | | | |
| 6.3 | Evidence Formats & Platforms | Windows, Linux, macOS, Android and iOS; RAW/DD, E01/Ex01, AFF/AFF4, VMDK, VHD/VHDX or equivalent. | | | |
| 6.4 | Evidence Integrity & Case Management | MD5, SHA-1, SHA-256 or stronger hashing, evidence verification, bookmarking/tagging, chain-of-custody, case management, investigation notes, audit trails and customizable forensic reports. | | | |
| 6.5 | Enterprise Integration | SIEM/XDR, Incident & Case Management, Threat Intelligence Platform, Malware Sandbox, Cyber Range and SAN/NAS evidence storage through APIs, IOC/file exchange or equivalent. | | | |
| 6.6 | Licensing, Security & Support | Appropriate multi-user/concurrent licensing, centralized license/user management and RBAC; all software/licenses, installation, configuration, integration, testing/UAT, training, documentation | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | and 5-year comprehensive updates/upgrades/support. | | | |
| 7 | Cyber Range Scenarios & Exercises | Cyber Range simulations, Red Team, Blue Team, Purple Team, CTF, Tabletop, Cyber Crisis, SOC, Incident Response, Digital Forensics, Malware Analysis and Threat Hunting exercises. | | | |
| **7.1** | Training & Capacity Building | Instructor-led and hands-on training covering Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Incident/Evidence Management, Digital/Mobile Forensics, Blockchain Investigation, servers, storage, virtualization, networks, firewall and associated ICT/security solutions. | | | |
| **7.2** | Research & Analysis Tools | Cybersecurity research, OSINT, threat research, data correlation, link/relationship analysis, timeline and graph analysis, visualization, dashboards and intelligence analysis, with AI/ML-assisted analytics where applicable. | | | |
| **7.3** | Integration | Integration with Cyber Range, SIEM/XDR, Threat Intelligence, Digital Forensics, Incident & Evidence Management and other project platforms through APIs/interfaces. | | | |
| **7.4** | Training Content & Knowledge Transfer | Training manuals, SOPs, administrator/user guides, laboratory exercises, scenarios, presentations, case studies, assessments | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | and Train-the-Trainer (ToT), including refresher/advanced training during support period. | | | |
| **7.5** | Implementation Model & Support | Training/scenarios and research tools shall be provided module-wise and as required by the Department; licensing, customization, configuration, updates and technical support shall be included. | | | |
| 8 | Platform | Enterprise web-based Application & Infrastructure Monitoring Dashboard Platform with centralized administration and management. | | | |
| 8.1 | Monitoring Capability | Centralized monitoring of applications/APM, servers, databases, networks, storage, virtualization, cloud infrastructure and endpoints. | | | |
| 8.2 | Dashboard & Analytics | Real-time interactive dashboards, customizable widgets, KPI monitoring, reports, analytics, alerts, notifications, historical data and trend analysis. | | | |
| 8.3 | Infrastructure Integration | Windows, Linux, VMware/Hyper-V, Docker/containers, databases, storage, network/security devices, SNMP, Syslog, WMI and REST APIs. | | | |
| 8.4 | Enterprise Integration | AD/LDAP, Cyber Range, SIEM/XDR, SAN/NAS, servers, network infrastructure and departmental applications/platforms. | | | |
| 8.5 | IT Operations & | Workflow automation, asset inventory, | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | Automation | configuration management, SLA monitoring, helpdesk/ticketing integration and ITSM capabilities. | | | |
| 8.6 | Alerts & Reporting | Threshold/event alerts, scheduled reports, email/SMS or equivalent notifications, performance analysis and capacity/trend reporting. | | | |
| 8.7 | Security | RBAC, centralized authentication, SSL/TLS encryption, audit logging and backup/restore. | | | |
| 8.8 | Solution Model | Zoho/ManageEngine or equivalent enterprise platform meeting/exceeding the specified requirements. | | | |
| 8.9 | Licensing | All required licenses/subscriptions, connectors, monitoring agents, APIs and management components. | | | |
| 8.10 | Implementation | Supply, installation, configuration, customization, integration, testing, UAT and commissioning. | | | |
| 8.11 | Documentation & Training | Architecture/configuration documentation, SOPs, administrator training, user training and knowledge transfer. | | | |
| 8.12 | Support | Minimum 5 years comprehensive software support including updates, upgrades, security patches and technical assistance. | | | |
| 9 | Type | Enterprise high-performance workstation with integrated ergonomic command/operator console suitable for SOC, Cyber Range, Red/Blue/Purple | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | Team and advanced cyber-security operations. | | | |
| 9.1 | Processor | Intel Core i9 current/latest generation or equivalent/better. | | | |
| 9.2 | Memory | Minimum 64GB DDR5 RAM, expandable to minimum 128 GB or higher. | | | |
| 9.3 | Storage | Minimum 2 TB PCIe Gen4 NVMe SSD with provision for additional internal storage. | | | |
| 9.4 | Graphics | Professional-grade dedicated GPU with adequate compute performance and memory capacity to support Cyber Security, SOC, Cyber Range, security analytics and multiple high-resolution display workloads. | | | |
| 9.5 | Displays | Dual 27-inch or higher IPS/QHD displays, anti-glare, with suitable dual-monitor mounting. | | | |
| 9.6 | Networking | Minimum 2.5 GbE Ethernet, Wi-Fi 6E or better and Bluetooth. | | | |
| 9.7 | Operating System | Windows 11 Pro 64-bit or equivalent professional OS, with Linux/virtualization support. | | | |
| 9.8 | Software Compatibility | Cyber Range, virtualization, SIEM/XDR, SOC monitoring, packet/network analysis, threat intelligence, security analysis and remote administration tools. | | | |
| 9.9 | Security | TPM 2.0, Secure Boot, BIOS/UEFI security, BitLocker/drive encryption support, endpoint protection and centralized management. | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| 9.10 | Integration | Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Video Wall, AD/LDAP and centralized authentication. | | | |
| 9.11 | Command Console | Professional ergonomic operator/command console with dual-monitor mounts, concealed cable management, power/data provisions and equipment/storage space. | | | |
| 9.12 | Peripherals | Professional keyboard/mouse, USB headset with microphone, Full-HD or better webcam and all necessary cables/adapters/accessories. | | | |
| 9.13 | Installation | Complete supply, installation, configuration, integration, testing and commissioning. | | | |
| 9.14 | Warranty | Minimum 5-year comprehensive onsite OEM warranty and technical support. | | | |

- **Eligibility Criteria**

| Sl. No | Eligibility Criterion | Supporting Document |
|---|---|---|
| 1 | Bidder must be registered in India and have been in operations for minimum 3 years as on bid opening. | GST Registration Certificate and PAN or COI |
| 2 | Average annual turnover of at least ₹10 Crores from IT Infrastructure business during last 3 financial years. | Audited financial statements for last 3 FYs |
| 3 | Bidder must not have been blacklisted, debarred or suspended by any Central/State Government or PSU during last 3 years. | Undertaking on company letterhead signed by Authorized Signatory |
| 4 | Positive net worth for each of last 3 financial years. | Audited Balance Sheet and/or CA Certificate |
| 5 | Bidder must be authorized reseller/partner for all quoted products and solutions. | Manufacturer Authorization Form specific to this tender |
| 6 | OEM from a country sharing land border with India | Supporting registration |

| Sl. No | Eligibility Criterion | Supporting Document |
|---|---|---|
| | eligible only if registered with competent authority as per applicable Government of India order. | documents |
| 7 | OEM undertaking that offered items are not nearing end-of-life/end-of-support until end of warranty. | Supporting undertaking/document |
| 8 | Project Experience: The bidder shall have successfully executed similar Enterprise Cyber Security Software projects during the last five (5) years and shall meet any one of the prescribed experience routes. Experience in Cyber Range/Cyber Training Platforms, SIEM/XDR, Threat Intelligence, AI/ML-based Cyber Security Analytics, Malware Analysis, Digital Forensics, Incident/Case/Digital Evidence Management, Cyber Security Research Platforms, or integration/customization of Enterprise Cyber Security Software solutions shall be considered relevant. Experience in any one or more of these categories shall be sufficient and the bidder shall not be required to demonstrate experience in all categories. | PO copies and completion reports |
| 9 | Mandatory pre-bid participation and site visit; written consent after pre-bid and Site Visit Certificate with Technical Bid. | Pre-bid/site visit documents and certificate |

- **Pre-Bid Meeting**

Participation in the pre-bid discussion is compulsory/mandatory through offline/online mode. Offers/bids of service providers who do not participate may not be considered for further evaluation, as stated in the source tender.

After attending the pre-bid discussion, the service provider shall submit written consent confirming understanding of the terms and quantum of work.

- **Commercial Conditions & Payment Terms**

Bids shall be submitted online through the Kerala e-GP system. Two covers are prescribed: (i) Technical Bid and (ii) Financial Bid. Foreign equipment rates shall be quoted in Indian Rupees.

| Source Payment Provision | Draft Status |
|---|---|
| Payment Clause | Payment will be released only after successful completion of supply, installation, configuration and commissioning of the project.<br>Request for advance payment, if any, will be considered as per rules, on request from the supplier and against submission of a valid Bank Guarantee. |

- **Other Payment Terms**

1. PBG shall be in favour of the Director General of Police, Kerala State.
2. PBG shall remain valid for contract period + 3 months.
3. Advance shall be adjusted in subsequent bills.
4. No advance without Bank Guarantee as per KFC Rule 182A & KSPM Clause 15.15.

- **General Conditions**

- ✓ Department reserves the right to accept or reject any/all bids, in full or in part, without assigning a reason. Contract may be awarded to the lowest evaluated bidder or a technically qualified firm whose proposal is considered most advantageous.
- ✓ Strict confidentiality of all departmental data, systems and information shall be maintained.
- ✓ No departmental data or information shall be copied, transferred or exported outside India under any circumstances.
- ✓ Selected firm shall commence work immediately upon issue of Work Order and signing of Agreement.
- ✓ Subcontracting is permitted only with prior written approval of the Department.
- ✓ Penalties/liquidated damages shall apply for delays, non-performance or breach as per rules.
- ✓ Bidders may propose equivalent or superior items, subject to technical evaluation and Department approval.
- ✓ Department decision on bid evaluation, award and execution shall be final and binding.
- ✓ OEM/Solution Provider shall submit duly filled compliance statement as prescribed. Non-submission may lead to rejection.
- ✓ Quoted items shall not be declared End of Sale for the next five years from bid submission.

- **Mode of Submission and e-Tender Conditions**

1. Online submission only through the Kerala e-GP website.
2. Two covers: Technical Bid and Financial Bid.
3. Foreign equipment rates shall be quoted in Indian Rupees.
4. Tender documents shall be downloaded only during the notified period.
5. Digitally signed tender and specified documents shall be uploaded before the last date/time.
6. Tender fee shall be paid online; non-payment may result in outright rejection.
7. EMD shall be paid online. Eligible SPD Kerala/National Small Scale Industries Corporation registered bidders may claim exemption with valid documentary proof.
8. Withdrawal and re-submission are permitted only until the last date/time for submission.
9. Bids shall be opened online at the Office of State Police Chief, Police Headquarters, Thiruvananthapuram.
10. Financial bids of technically qualified tenderers only shall be considered for opening.
11. All tenderers quoting the items shall be ready for technical evaluation at Thiruvananthapuram on the date intimated by the Department.
12. Hard copies of relevant tender documents shall be produced at technical evaluation when required.

13. Uploaded documents shall bear signature/office seal of bidder/authorized person and shall be digitally signed.
14. Bidders shall ensure compliance with Digital Signature Certificate requirements and e-GP procedures.

- **Testing, Documentation, Commissioning & Knowledge Transfer**

15. Installation testing
16. Configuration validation
17. Functional testing
18. Integration testing
19. Security validation
20. Performance testing
21. User Acceptance Testing (UAT)
22. Final commissioning
23. System Architecture Documentation
24. Configuration Documents
25. Administrator Manuals
26. User Manuals
27. Standard Operating Procedures (SOPs)
28. API Documentation
29. License Documentation
30. Test Reports
31. Commissioning Reports
32. As-built Documentation
33. Training manuals, hands-on sessions and knowledge transfer documentation

- **Training & Knowledge Transfer**

34. Platform Administration
35. User Administration
36. Security Operations
37. Threat Detection & Investigation
38. Malware Analysis
39. Incident Management
40. Digital Forensic Operations
41. Reporting & Dashboard Management
42. Backup & Recovery
43. Preventive Maintenance
44. Basic Troubleshooting
45. Administrator and user training
46. Hands-on sessions, manuals, guides and knowledge transfer

- **Warranty, Support & Maintenance**

47. All applicable software licenses, subscriptions and activation keys shall be supplied.
48. Five (5) years comprehensive OEM/software support or as specified in the BOQ.
49. Software updates, security patches and version upgrades during the support period.
50. Remote and onsite technical support, as applicable.

51. Bug fixes, troubleshooting and incident resolution.
52. Coordination with OEMs for issue resolution.
53. Maintenance of the complete integrated software environment throughout the contract period.
54. Module-specific support requirements in the technical specifications shall also apply.

- **Bidder Compliance Declaration**

We hereby certify that the information and technical compliance statements submitted with this bid are true and complete. All deviations, limitations, dependencies, licensing restrictions and assumptions have been explicitly disclosed.

| Declaration | Bidder Entry |
|---|---|
| Bidder Name | |
| Authorized Signatory | |
| Designation | |
| Date | |
| Place | |
| Company Seal | |
| Overall Technical Compliance | COMPLIED / PARTIALLY COMPLIED / NOT COMPLIED |
| Commercial Compliance | COMPLIED / DEVIATION |
| Deviation Schedule Attached | YES / NO |

- **Deviation / Exception Schedule**

Any deviation from a minimum requirement must be listed here. If there are no deviations, the bidder shall write 'NIL'.

| Sl. | Tender Section / Clause | Tender Requirement | Bidder's Deviation / Exception | Impact | Department Decision |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |

- **Compliance Status Legend**

| Status | Meaning |
|---|---|
| COMPLIED | Bidder fully meets or exceeds the stated minimum requirement. |
| PARTIALLY COMPLIED | Bidder meets part of the requirement but has a stated limitation or gap. |
| NOT COMPLIED | Bidder does not meet the requirement. |
| DEVIATION | Bidder proposes an alternative or departure requiring Department evaluation/approval. |
| NOT APPLICABLE | Requirement genuinely does not apply; bidder must provide justification. |

- **Overall Responsibility of the Selected Bidder**

The selected bidder shall be responsible for the complete end-to-end delivery, implementation and operationalization of the proposed Enterprise Cyber Security Software Solution(s), covering one or more of the specified solution areas, including:

- ✓ Supply / licensing of proprietary software or provision of open-source software components, as applicable.
- ✓ Installation, configuration and customization of the proposed software solutions.
- ✓ Integration and interoperability with the existing and proposed Cyber Operations infrastructure and other relevant departmental systems.
- ✓ Development and implementation of required APIs, connectors, interfaces, workflows, dashboards and reports.
- ✓ Testing, security validation, User Acceptance Testing (UAT), commissioning and performance validation.
- ✓ Provision of all required implementation tools, middleware, connectors, documentation and technical components necessary for successful deployment.
- ✓ Administrator training, user training, Train-the-Trainer (ToT) and knowledge transfer.
- ✓ Preparation and submission of system architecture, configuration documents, user manuals, administrator manuals and SOPs.
- ✓ Provision of applicable software updates, upgrades, security patches, bug fixes and technical support during the contract/support period.
- ✓ Provision of warranty and comprehensive support and maintenance as specified in the RFP.

The bidder shall ensure that all proposed software components are fully functional, interoperable, secure, scalable and operational upon completion of the implementation. All necessary licenses, subscriptions, APIs, connectors, customization, integration services, documentation, training and other associated requirements shall be clearly identified and quoted in the Commercial Bid/BOQ, wherever applicable. **The entire project cost should be quoted in the BOQ as a whole.**

- **Contact for Clarifications**

  Cyber Operations Wing, Kerala Police

  Email: cyberops-sec.pol@kerala.gov.in

  Clarifications should be submitted well in advance of the bid submission deadline.

  Source contact / technical clarification reference: Assistant Sub Inspector of Police, Cyber Security and Advanced Crimes, Cyber Operations, PHQ, telephone 9895258496.

- **General Conditions**

1. Right of the Department: The Department reserves the right to accept or reject any or all bids, in whole or in part, and to modify or cancel the tender process in accordance with applicable Government rules.
2. Quantity/Scope Variation: The Department may increase, decrease, omit or combine items/quantities within the approved budget and as permitted under applicable procurement rules.
3. Confidentiality: The bidder shall maintain strict confidentiality of all departmental data, systems, documents, credentials and information.

4. Data Residency: Departmental data and information shall remain within India and shall not be transferred or stored outside India without prior written approval of the Department and as permitted by applicable rules.
5. Commencement: The successful bidder shall commence work within the period specified in the Work Order/Agreement.
6. Subcontracting: Subcontracting shall be permitted only with prior written approval of the Department. The bidder shall remain fully responsible for the contracted work.
7. Penalty/LD: Liquidated damages, penalties or other contractual remedies shall apply for delay, non-performance or breach as specified in the RFP/SLA.
8. Equivalent Solutions: Bidders may offer equivalent or higher-performing products/solutions meeting the prescribed minimum requirements, subject to technical evaluation and approval.
9. Technical Compliance: A duly completed and digitally signed Technical Compliance Statement shall be submitted in the prescribed format. Non-submission may result in rejection.
10. Product Lifecycle: Offered proprietary products/solutions shall not be End-of-Sale/End-of-Life at the time of bidding and shall have OEM support, updates and security patches for the required contract period.
11. Online Submission: All bids shall be submitted online only through the Kerala e-GP portal in the prescribed covers. No other mode of submission shall be accepted.
12. Bid Covers: The e-Tender shall be submitted in two covers – Technical Bid and Financial Bid, as specified in the e-GP portal.
13. Tender Fee & EMD: Tender fee and EMD, wherever applicable, shall be remitted online through the e-GP portal. Valid exemptions shall be supported by required documents.
14. Withdrawal/Resubmission: Bids may be withdrawn or resubmitted through the e-GP portal up to the prescribed closing date and time.
15. Bid Opening: Bids shall be opened electronically through the e-GP portal on the date and time specified in the tender. Only technically qualified bidders shall proceed to financial evaluation.
16. Technical Evaluation: The Technical Evaluation Committee may evaluate compliance, experience, OEM documentation, demonstrations/PoC, technical presentations and other requirements specified in the RFP.
17. Document Verification: The Department may require original/certified copies of uploaded documents for verification.
18. Clarifications: Bidders shall seek clarifications through the prescribed e-GP mechanism within the specified period. Only official clarifications/corrigenda issued by the Department shall be binding.
19. Digital Signature: Bidders shall possess a valid Digital Signature Certificate (DSC) and digitally sign documents as required by the e-GP system.
20. SLA: The successful bidder shall execute the prescribed Service Level Agreement (SLA) covering support, response/resolution times, escalation, availability and applicable penalties.
21. Decision of Department: Decisions of the Department/competent authority shall be governed by the tender conditions and applicable Government procurement rules.
22. The selected firm shall complete the delivery, installation, configuration and commissioning of all items listed in the annexures within **Ninety Days (90) days** from the date of issue of Work Order/Supply Order.

- **Note to Bidders:-**

1. Bidders have to procure legally valid Digital Certificate (Class III) as per Information

Technology Act, 2000 for digitally signing their electronic bids. Bidders can procure the same from any of the license certifying authority of India. For more details, please visit the e-GP website www.etenders.kerala.gov.in

2. Bidders are advised to note the Tender Id and Tender No. & Date for future reference.

3. All uploaded documents should contain the signature and the office seal of the bidder/authorized persons and should be digitally signed while uploading. Documents uploaded without digitally signing shall entitle rejection of the tender.

4. In the case of Foreign Equipment, the rate should be quoted in Indian Rupees. Preference will be given to those who are ready to supply the item without opening Letter of Credit. Ordinarily, no advance payment will be made for procuring the above item.

v). For obtaining Digital Signature Certificate and help on etendering process, contact Kerala State IT Mission, eGovernment Procurement PMU & Help desk, Basement floor of Pension Treasury Building, Uppalam Road, Statue, Thiruvananthapuram; Ph :0471-2577088, 2577 IBB; Toll free no: 18002337315; e- mail:etendershelo@kerala.gov. in; Website: www.etenders.kerala.gov.in on all government working days from 9:30 am to 5:30 pm.

vi). Successful bidder should execute a service level agreement format available at the Office of IGP Cyber Operations, Pattom Thiruvananthapuram. Cost of stamp paper for SLA is one rupee for every rupee 1000 or part thereof on the amount agreed in the contract, subject to a minimum of rupees 200 and a maximum of rupees one lakh.

Vii)**. Contact for Clarifications**

**For any clarifications regarding this tender, bidders may contact the Cyber Operations Wing, Kerala Police:**

- **Email:** "cyberops-sec.pol@kerala.gov.in"

All queries should be sent well in advance of the bid submission deadline to ensure a response in time.

**NOTE:-BIDDERS ARE ADVISED TO GO THROUGH THE CONDITIONS IN THE NOTICE INVITING TENDER AND THE TENDER DOCUMENT CAREFULLY AND COMPLY WITH THEM TO AVOIDOUTRIGHT REJECTION OF THEIR TENDER.**

**Bidders are requested to make online payment of EMD and tender fee before 72 hours in advance of last date.**

For any litigation relating to this order, the jurisdiction will be Thiruvananthapuram City.

Sd/-
Assistant Inspector General of Police, Procurement
For DIRECTOR GENERAL OF POLICE &
STATE POLICE CHIEF, KERALA

# Scope of work and specification

The scope of work includes the design, supply, installation, configuration, customization, integration, testing, training, commissioning and **five (5)** years of comprehensive support and maintenance for an integrated enterprise cyber capability infrastructure comprising Cyber Range Software, AI-Driven Threat Analytics Platform, Threat Intelligence Platform, Digital Forensics Solutions, Incident Management System, Cyber Security Solutions, enterprise servers, storage systems, networking, security appliances, and all associated hardware, software, and supporting infrastructure, in accordance with the Technical Specifications, Bill of Quantities (BoQ) and tender conditions.

## Scope of Work

The project shall be established at the 2nd Floor, Police Training College, under the Scheme of ASUMP 2026–2027, and shall include complete end-to-end supply, licensing, installation, configuration, customization, integration, testing, User Acceptance Testing (UAT), commissioning, documentation, training, knowledge transfer, warranty and comprehensive technical support.

The scope shall cover the complete integrated Cyber Range and Cyber Security ecosystem, comprising the specified Cyber Range/SIEM-XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Incident/Case and Evidence Management, Digital Forensics, Cyber Security Training/Research, IT Operations Monitoring and Cyber Security/AI Workstations, including all necessary hardware, software, licences/subscriptions, APIs, connectors, accessories and implementation components required for the successful implementation, integration and operation of the complete solution.

The solution shall be modular, scalable, interoperable and technology-neutral. The bidder may propose Proprietary/Commercial, Customized Open-Source or Hybrid solutions, provided that all specified functional, technical, security, performance, scalability, integration and support requirements are fully met. Equivalent or superior technologies, products, platforms and frameworks providing comparable or better functionality and meeting the prescribed requirements shall be acceptable.

For Proprietary/Commercial, Open-Source and Hybrid solutions, the bidder shall be fully responsible for all required customization, configuration, integration, security hardening,

development, licensing/subscriptions, maintenance, updates/upgrades and technical support, as applicable, without any reduction in the mandatory scope or functionality.

For Open-Source or Hybrid solutions, the bidder shall additionally be responsible for all customization, integration, security hardening, development, maintenance, updates/upgrades and technical support necessary to deliver a complete, secure and fully functional enterprise solution. The use of Open-Source components shall not result in any reduction in the mandatory scope, functionality, security, performance, scalability, interoperability or support requirements.

Where Open-Source components are proposed, the bidder shall have demonstrated capability and relevant experience in their enterprise deployment, customization, integration, maintenance and support, and shall provide the necessary customer references and documentary evidence.

The bidder shall submit a component-wise and year-wise cost breakup, clearly separating one-time and recurring costs, including licences/subscriptions, support/AMC, updates/upgrades, threat-intelligence feeds, connectors, customization, training and other applicable costs for Year 1 to Year 5, together with the cumulative Total Cost of Ownership (TCO).

The bidder shall demonstrate relevant experience in implementation of comparable Cyber Security, Cyber Range or integrated security solutions and shall provide details and documentary evidence of successfully installed/commissioned customer references, including customer name, work order/contract reference, scope, value, commissioning status and contact/reference details. Where Open-Source technologies are proposed, relevant experience in their customization and integration shall also be demonstrated.

The bidder shall be responsible for the complete integrated solution as a single point of responsibility, irrespective of the combination of Commercial, Open-Source or Hybrid components proposed. The prime bidder shall remain fully responsible for the performance, integration, interoperability and support of all OEM products, software, Open-Source components, specialist technologies and implementation partners engaged for the project.

The bidder may engage appropriate OEMs and/or specialist implementation partners, subject to the eligibility, subcontracting and prior-approval provisions of the tender, wherever applicable. Such engagement shall not dilute or transfer the prime bidder's responsibility for the complete Scope of Work, deliverables, performance, integration, warranty, support or contractual obligations.

The Department may require technical demonstration/Proof of Concept (PoC) during technical evaluation and may verify the customer references and credentials submitted by

the bidder. Where a demonstration/PoC is required, it shall be conducted in accordance with the uniform evaluation methodology, requirements and criteria prescribed in the tender.

All components necessary to meet the specified functional, technical, security, performance, scalability and integration requirements shall be deemed to form part of the bidder's complete solution, irrespective of whether such components are individually identified in the BOQ, provided such components are essential for delivering the specified functionality of the complete integrated solution.

- **Integrated Technical Scope / BOQ**

| Sl. | Technical Item | Core Scope |
|---|---|---|
| 1 | Enterprise Cyber Range Simulation, Training & Integrated SIEM/XDR Platform | Cyber Range, virtualization, SIEM/XDR, SOC analytics, orchestration, training and integration |
| 2 | Enterprise AI/ML Threat Analytics, Security Analytics & Threat Hunting Platform | AI/ML analytics layer on Department-provided AI/GPU infrastructure |
| 3 | Enterprise Threat Intelligence Platform (TIP) | IOC/TTP intelligence, feeds, enrichment, standards and API integration |
| 4 | Enterprise Malware Sandbox Appliance | Dedicated malware analysis, detonation, behavioural analysis and intelligence integration |
| 5 | Incident, Case & Digital Evidence Management and Security Response Workflow | Incident/case lifecycle, evidence management, chain of custody and response workflows |
| 6 | Enterprise Digital Forensic Analysis & Investigation Software Suite | Computer, mobile, memory, network and multimedia forensics |
| 7 | Cyber Range Scenarios, Cyber Security Training, Research, Capacity Building & Advanced Analysis | Training, exercises, research tools, OSINT, analysis and knowledge transfer |
| 8 | Enterprise Application, Infrastructure & IT Operations Monitoring Dashboard Platform | APM, servers, databases, networks, storage, virtualization, cloud, endpoints and ITSM |
| 9 | Enterprise High-Performance Cyber Security Workstation with Integrated Command Console | SOC/Cyber Range operator workstation, dual displays, console and peripherals |

- **Detailed Technical Specifications**

### 2.1 Enterprise Cyber Range Simulation, Training & Integrated SIEM/XDR Platform

| Parameter | Minimum Technical Requirement |
|---|---|
| Platform | Enterprise Cyber Range supporting ILT, practical labs, CTF, Red/Blue/Purple Team, attack simulation, Incident Response, Malware Analysis, Digital Forensics, SOC training, Cyber Crisis/Tabletop exercises and competency assessments. |
| Capacity | Minimum 200 concurrent trainees, 20 instructors, 300+ VMs, 10+ concurrent labs and 100+ scenarios, with minimum 50% future scalability. |

| Parameter | Minimum Technical Requirement |
|---|---|
| Virtualization | VMware vSphere / Hyper-V / Proxmox VE Enterprise / KVM/OpenStack or equivalent with HA, clustering, live migration, templates, snapshots/rollback, monitoring and API integration. |
| Range Management | Centralized web-based orchestration supporting automated VM/network provisioning, isolated environments, lab/scenario deployment, cloning, snapshots, rollback, automated reset, team management and scoring. |
| SIEM/XDR | Enterprise SIEM/XDR using Wazuh with OpenSearch or equivalent, supporting minimum 250 monitored assets, centralized log/event collection, correlation, alerting, threat detection and security analytics. |
| Threat & SOC Analytics | IOC matching, MITRE ATT&CK mapping, UEBA, FIM, vulnerability detection, threat hunting, risk-based alerting, SOC dashboards, reporting, incident/case management and workflow automation. |
| Integration | AD/LDAP, firewalls, IDS/IPS, DNS/DHCP, Suricata, Zeek, MISP, Malware Sandbox, Threat Intelligence, AI/ML Threat Analytics, SAN/NAS, Video Wall, IFMS and other enterprise/security infrastructure through standard interfaces/APIs. |
| Security | RBAC, MFA, SSL/TLS, audit logging, centralized authentication, backup and recovery. |
| Solution Model & Pricing | Proprietary/Commercial, Open-Source or Hybrid. Proprietary and Open-Source options shall be separately priced, including implementation, licenses/subscriptions and 5-year TCO. |
| Training | Minimum 15 working days Administrator Training + 20 working days Instructor Training, including scenario/lab development and Red/Blue/Purple Team, CTF, SOC and Incident Response exercises. |
| Implementation | Complete installation, configuration, customization, integration, testing, performance validation, UAT, commissioning, documentation, SOPs and knowledge transfer. |
| Support | Minimum 5 years comprehensive support, including software/security updates, patches, scenario updates, technical assistance and capacity building. |

2.2 Enterprise AI/ML Threat Analytics, Security Analytics & Threat Hunting Platform

| Parameter | Minimum Technical Requirement |
|---|---|
| Platform | Enterprise AI/ML-based Threat Analytics and Security Monitoring Platform, deployed on Department-provided AI/GPU Compute Servers and on-premises Data Centre infrastructure. |
| Architecture | AI/ML analytics layer integrated with the Cyber Range and SIEM/XDR platform; shall not require procurement/deployment of a duplicate SIEM/XDR environment. |
| AI/ML Framework | TensorFlow, PyTorch, Scikit-learn, MLflow, JupyterLab or equivalent enterprise AI/ML frameworks/tools. |
| AI Security Analytics | AI-assisted threat detection, anomaly detection, UEBA, behavioural analytics, predictive threat analytics, threat hunting, malware analytics, IOC correlation, MITRE ATT&CK mapping and risk scoring. |
| Data Sources | Windows, Linux, AD, firewalls, IDS/IPS, DNS, Syslog, NetFlow/IPFIX, Zeek, Suricata, Sysmon, PCAP and Cyber Range exercises. |

| Parameter | Minimum Technical Requirement |
|---|---|
| SIEM/XDR Integration | Full integration with Wazuh/OpenSearch or equivalent SIEM/XDR for logs, alerts, IOCs, risk scores and AI-generated threat intelligence. |
| Malware & Threat Intelligence | Integration with Enterprise Malware Sandbox and Threat Intelligence Platform for behavioural analysis, IOC extraction, correlation and threat-intelligence enrichment. |
| Custom AI/ML Development | Development/customization of AI/ML security use cases, models, detection rules, correlation rules, dashboards, automated reports and threat-hunting workflows. |
| Deployment & APIs | Containerized deployment using Docker or equivalent with REST API/standard interfaces. |
| Security | RBAC, SSL/TLS encryption, audit logging, secure authentication, backup and recovery. |
| Hardware Scope | Department-provided AI/GPU Compute Infrastructure. AI/GPU server hardware is excluded from this BOQ item unless specifically stated otherwise. |
| Implementation & Training | Installation, configuration, customization, integration, testing, UAT, administrator/SOC analyst training, documentation, SOPs, architecture diagrams and knowledge transfer. |
| Support | Minimum 5 years comprehensive software support, including upgrades, security patches, remote/onsite technical assistance and AI/ML solution support. |

2.3 Enterprise Threat Intelligence Platform (TIP)

| Parameter | Minimum Technical Requirement |
|---|---|
| Platform & Intelligence | Enterprise web-based TIP supporting centralized aggregation, correlation and management of IOCs, TTPs, malware, phishing, ransomware, botnet and vulnerability intelligence, with automated ingestion, enrichment, reputation analysis, threat scoring and campaign tracking. |
| Standards & Integration | STIX/TAXII, OpenIOC, YARA, Sigma, MITRE ATT&CK, CVE/NVD and MISP or equivalent; API integration with Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Malware Sandbox, Suricata, Zeek, Firewalls, EDR/XDR and other security infrastructure. |
| Management, Licensing & Support | IOC search, threat hunting, dashboards, alerts, reporting, intelligence sharing, RBAC, SSL/TLS, audit logging and backup/recovery. Include software licenses, threat-intelligence feeds and connectors, installation, integration, UAT, documentation, training and 5-year comprehensive updates and technical support. |

2.4 Enterprise Malware Sandbox Appliance

| Parameter | Minimum Technical Requirement |
|---|---|
| Appliance & Malware Analysis | Dedicated Malware Sandbox Appliance with minimum 16 CPU cores, 64 GB RAM, 2 × 960 GB Enterprise SSD in RAID-1, minimum 4 TB analysis storage and redundant power supplies. Static, dynamic and behavioural analysis, detonation, exploit/ransomware/zero-day detection and AI-assisted threat classification. |
| Threat Analysis & Intelligence | Windows, Linux, Android and macOS-related files/workloads, executables, scripts, PDF/Office documents, archives, email attachments and web downloads; automated IOC extraction, |

| | |
|---|---|
| | malware reports, MITRE ATT&CK mapping, threat scoring and signature/detection-artifact generation. |
| Integration | SIEM/XDR, NGFW, Threat Intelligence Platform, AI/ML Threat Analytics, Cyber Range, Email Security Gateway, WAF and other security infrastructure, including automated sample submission and verdict/IOC exchange. |
| Management, Licensing & Support | Centralized web management, RBAC, SSL/TLS, audit logging and reporting. Include all hardware, software, licenses, subscriptions, threat-intelligence updates and accessories, installation, integration, testing/UAT, documentation, administrator training and 5-year comprehensive onsite OEM warranty, updates and technical support. |

2.5 Incident, Case & Digital Evidence Management and Security Response Workflow

| Parameter | Minimum Technical Requirement |
|---|---|
| Incident & Case Management | Centralized incident registration, categorization, prioritization, assignment, escalation, investigation, case notes, approvals and complete incident/case lifecycle tracking. |
| Security Response Workflow | Configurable workflows for alert triage, task assignment, escalation, SLA tracking, investigation, containment, remediation, recovery and incident closure. |
| Digital Evidence Management | Centralized registration and management of digital evidence, evidence inventory, evidence assignment, QR/barcode identification, secure evidence attachment/storage and forensic workflow tracking. |
| Evidence Integrity & Chain of Custody | MD5, SHA-256 or stronger hashing, evidence integrity validation, chain-of-custody tracking, version control and complete audit trail. |
| Integration | SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence Platform, Malware Sandbox, Digital Forensic Software/Mobile Forensic Tools, Cyber Range, AD/LDAP and SAN/NAS evidence storage. |
| Dashboard & Reporting | Real-time incident/case/evidence status, severity, response time, SLA compliance, trends, KPIs, evidence tracking, audit trails and management/executive/forensic reports. |
| Security & Access | RBAC, MFA, SSL/TLS, centralized authentication, audit logging, secure API access, backup and recovery. |
| Implementation & Support | Installation/deployment, configuration, customization, integration, testing/UAT, documentation, administrator/user training and 5-year comprehensive software updates, maintenance and technical support. |

2.6 Enterprise Digital Forensic Analysis & Investigation Software Suite

| Parameter | Minimum Technical Requirement |
|---|---|
| Forensic Analysis Capability | Computer, Mobile, Memory, Network and Multimedia Forensic Analysis, including file-system analysis, deleted-file recovery, registry, email/browser artefacts, timeline analysis, memory forensics, malware-related artefact analysis and forensic reporting. |
| Evidence Acquisition & Mobile Forensics | Logical, file-system and physical acquisition where technically supported; disk/image acquisition and compatibility with forensic imaging appliances and hardware write-blocking/acquisition kits; Android and iOS mobile forensic acquisition/analysis where supported. |

| Parameter | Minimum Technical Requirement |
|---|---|
| Image & Video Forensics | Enhancement, deblurring, frame-level analysis, authentication/integrity examination, object tracking, metadata extraction and relevant multimedia forensic analysis. |
| Evidence Formats & Platforms | Windows, Linux, macOS, Android and iOS; RAW/DD, E01/Ex01, AFF/AFF4, VMDK, VHD/VHDX or equivalent. |
| Evidence Integrity & Case Management | MD5, SHA-1, SHA-256 or stronger hashing, evidence verification, bookmarking/tagging, chain-of-custody, case management, investigation notes, audit trails and customizable forensic reports. |
| Enterprise Integration | SIEM/XDR, Incident & Case Management, Threat Intelligence Platform, Malware Sandbox, Cyber Range and SAN/NAS evidence storage through APIs, IOC/file exchange or equivalent. |
| Licensing, Security & Support | Appropriate multi-user/concurrent licensing, centralized license/user management and RBAC; all software/licenses, installation, configuration, integration, testing/UAT, training, documentation and 5-year comprehensive updates/upgrades/support. |

2.7 Cyber Range Scenarios, Cyber Security Training, Research, Capacity Building & Advanced Analysis

| Parameter | Minimum Technical Requirement |
|---|---|
| Cyber Range Scenarios & Exercises | Cyber Range simulations, Red Team, Blue Team, Purple Team, CTF, Tabletop, Cyber Crisis, SOC, Incident Response, Digital Forensics, Malware Analysis and Threat Hunting exercises. |
| Training & Capacity Building | Instructor-led and hands-on training covering Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Incident/Evidence Management, Digital/Mobile Forensics, Blockchain Investigation, servers, storage, virtualization, networks, firewall and associated ICT/security solutions. |
| Research & Analysis Tools | Cybersecurity research, OSINT, threat research, data correlation, link/relationship analysis, timeline and graph analysis, visualization, dashboards and intelligence analysis, with AI/ML-assisted analytics where applicable. |
| Integration | Integration with Cyber Range, SIEM/XDR, Threat Intelligence, Digital Forensics, Incident & Evidence Management and other project platforms through APIs/interfaces. |
| Training Content & Knowledge Transfer | Training manuals, SOPs, administrator/user guides, laboratory exercises, scenarios, presentations, case studies, assessments and Train-the-Trainer (ToT), including refresher/advanced training during support period. |
| Implementation Model & Support | Training/scenarios and research tools shall be provided module-wise and as required by the Department; licensing, customization, configuration, updates and technical support shall be included. |

2.8 Enterprise Application, Infrastructure & IT Operations Monitoring Dashboard Platform

| Parameter | Minimum Technical Requirement |
|---|---|
| Platform | Enterprise web-based Application & Infrastructure Monitoring Dashboard Platform with centralized administration and management. |
| Monitoring Capability | Centralized monitoring of applications/APM, servers, databases, networks, storage, virtualization, cloud infrastructure and endpoints. |

| Parameter | Minimum Technical Requirement |
|---|---|
| Dashboard & Analytics | Real-time interactive dashboards, customizable widgets, KPI monitoring, reports, analytics, alerts, notifications, historical data and trend analysis. |
| Infrastructure Integration | Windows, Linux, VMware/Hyper-V, Docker/containers, databases, storage, network/security devices, SNMP, Syslog, WMI and REST APIs. |
| Enterprise Integration | AD/LDAP, Cyber Range, SIEM/XDR, SAN/NAS, servers, network infrastructure and departmental applications/platforms. |
| IT Operations & Automation | Workflow automation, asset inventory, configuration management, SLA monitoring, helpdesk/ticketing integration and ITSM capabilities. |
| Alerts & Reporting | Threshold/event alerts, scheduled reports, email/SMS or equivalent notifications, performance analysis and capacity/trend reporting. |
| Security | RBAC, centralized authentication, SSL/TLS encryption, audit logging and backup/restore. |
| Solution Model | Zoho/ManageEngine or equivalent enterprise platform meeting/exceeding the specified requirements. |
| Licensing | All required licenses/subscriptions, connectors, monitoring agents, APIs and management components. |
| Implementation | Supply, installation, configuration, customization, integration, testing, UAT and commissioning. |
| Documentation & Training | Architecture/configuration documentation, SOPs, administrator training, user training and knowledge transfer. |
| Support | Minimum 5 years comprehensive software support including updates, upgrades, security patches and technical assistance. |

## 2.9 Enterprise High-Performance Cyber Security Workstation with Integrated Command Console

| Sl. No. | Feature | Minimum Technical Requirement |
|---|---|---|
| 1 | Type | Enterprise high-performance AI-enabled workstation/desktop AI appliance with integrated ergonomic operator/command console, suitable for SOC, Cyber Range, Red/Blue/Purple Team, AI/ML Threat Analytics, malware analysis, digital forensics and advanced cyber-security operations. |
| 2 | Make/Model | Product make and model shall be specified by the bidder. OEM technical datasheet shall be submitted along with the bid. Equivalent or superior products meeting all mandatory requirements shall be acceptable. |
| 3 | Monitor | Minimum 24-inch FHD IPS display, height-adjustable, with minimum 1 × HDMI and 1 × USB Type-C port. |
| 4 | Architecture | Architecture optimized for AI workloads, with tightly integrated CPU-GPU communication, high-bandwidth memory architecture and AI-focused compute capability suitable for local AI inference, model development and cyber-security analytics. |
| 5 | AI Compute Performance | Minimum 1 PFLOP / 1000 TFLOPS FP4 AI compute performance, or equivalent/superior AI inferencing capability. |
| 6 | AI Model Capacity – Single Node | The workstation shall support deployment/inference of AI models of up to 200 billion parameters on a single system, subject to the supported model framework and software environment. |
| 7 | AI Model Capacity – Two Node | The proposed architecture shall support AI models of up to 400 billion parameters using a two-node configuration, with the required high-speed interconnect and OEM-supported interconnect cables/accessories. |

| Sl. No. | Feature | Minimum Technical Requirement |
|---|---|---|
| 8 | Processor | AI-optimized processor architecture with minimum 20 CPU cores and integrated CPU-GPU architecture. NVIDIA GB10 or equivalent/superior architecture may be proposed. |
| 9 | CPU Cache | Minimum 16 MB L2 cache, or equivalent/superior processor cache architecture. |
| 10 | System Memory | Minimum 128 GB unified/coherent system memory or equivalent high-bandwidth memory architecture suitable for AI workloads. |
| 11 | Memory Architecture | Preference shall be given to unified or coherent memory architecture rather than fragmented CPU and GPU memory pools, provided the proposed architecture meets or exceeds the specified AI performance and capacity requirements. |
| 12 | Storage | Minimum 1 TB NVMe local storage, PCIe Gen4 or better, with provision for additional storage where required. |
| 13 | GPU / AI Accelerator | Enterprise AI GPU/accelerator based on NVIDIA Blackwell architecture or equivalent/superior technology, capable of meeting or exceeding the specified AI compute and model-capacity requirements. |
| 14 | Operating System | Linux-based AI-optimized operating system suitable for AI/ML workloads, containerized workloads, cybersecurity tools and enterprise management. Support for required virtualization/container technologies shall be provided. |
| 15 | Networking – Ethernet | Minimum 10GbE RJ-45 connectivity. |
| 16 | High-Speed Interconnect | Minimum 2 × QSFP high-speed ports, supporting aggregate/interconnect bandwidth of 200 Gbps or higher, or equivalent/superior high-speed node-to-node interconnect technology required for multi-node AI workloads. |
| 17 | Wireless Connectivity | Minimum Wi-Fi 6E or better and Bluetooth 5.4 or better, with integrated/internal antenna where applicable. |
| 18 | USB / I/O Ports | Minimum: 1 × USB 3.2 Gen 2x2 (20 Gbps) Type-C port with DisplayPort Alt Mode and power input; 3 × USB 3.2 Gen 2x2 (20 Gbps) Type-C ports with DisplayPort Alt Mode; and 1 × HDMI 2.1 or better port, or equivalent/superior I/O configuration. |
| 19 | Display Support | Shall support multiple high-resolution external displays suitable for SOC/Cyber Range operations and AI/cyber-security workflows. |
| 20 | Security | Minimum TPM 2.0, Secure Boot, hardware/firmware security controls, BIOS/UEFI security and storage encryption capability. |
| 21 | AI/ML Software Compatibility | Shall support enterprise AI/ML frameworks and tools including TensorFlow, PyTorch, Scikit-learn, MLflow, JupyterLab or equivalent, together with required GPU acceleration, containerization and development environments. |
| 22 | Cyber Security Software Compatibility | Shall support installation and operation of required Cyber Range, SIEM/XDR, SOC monitoring, packet/network analysis, Threat Intelligence, Malware Analysis, Digital Forensics, AI/ML Threat Analytics and security-analysis tools, subject to the respective software's platform requirements. |
| 23 | Integration | Shall support integration with Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Digital Forensics platforms, AD/LDAP, centralized authentication, network/security infrastructure and other approved enterprise systems through standard interfaces/APIs wherever applicable. |
| 24 | Virtualization / Containers | Shall support required virtualization and container technologies for deployment of approved Cyber Security, AI/ML and Cyber Range workloads, subject to the capabilities of the proposed platform. |
| 25 | Management | Enterprise-grade system monitoring, firmware/driver management, hardware health monitoring and centralized management capability shall be supported. |
| 26 | Command Console | Professional ergonomic operator/command console with dual/multi-monitor mounting provision, concealed cable management, power/data provisions and suitable equipment/storage space. |
| 27 | Seating | Heavy-duty, high-back ergonomic operator chair with adjustable height, lumbar support and adjustable armrests. |
| 28 | Peripherals | Professional keyboard and mouse, USB headset with microphone, Full-HD or better webcam, required power cables, display cables, adapters and all accessories necessary for complete operation. |
| 29 | AI Factory / Data- | Preference may be given to an OEM ecosystem capable of providing both the desktop |

| Sl. No. | Feature | Minimum Technical Requirement |
|---|---|---|
| | Centre Alignment | AI appliance/workstation and corresponding data-centre/server-scale AI infrastructure, enabling seamless transition from workstation-scale AI development/inference to server/cluster-scale deployment. This shall not restrict equivalent or superior solutions meeting the mandatory requirements. |
| 30 | Installation & Integration | Complete supply, installation, configuration, customization, integration, testing, performance validation, UAT and commissioning, including required drivers, firmware, software environment and approved security configuration. |
| 31 | Documentation | OEM technical datasheet, architecture documentation, configuration documentation, user/administrator manuals and relevant operational documentation shall be provided. |
| 32 | Warranty & Support | Minimum 5-year comprehensive onsite OEM warranty and technical support, including hardware defect rectification/replacement, applicable firmware/driver updates, technical assistance and support for the supplied platform. |
| 33 | High-Speed Interconnect Accessories | All OEM-recommended cables, QSFP modules, adapters, transceivers and accessories required for the specified two-node AI configuration shall be included. |
| 34 | Completeness | All hardware, software, licences, drivers, firmware, accessories, interconnects and implementation components necessary to achieve the specified functionality and performance shall be included in the bidder's complete solution. |

- **Technical Compliance Statement & Status**

The bidder shall submit a line-by-line compliance statement against every requirement. The bidder shall not merely state 'Complied'; supporting document reference, page number, model/part number, license type and deviation (if any) shall be stated wherever applicable.

Recommended status values: COMPLIED / PARTIALLY COMPLIED / NOT COMPLIED / DEVIATION / NOT APPLICABLE. Any deviation from a minimum requirement shall be explicitly declared. Silence or blank status may be treated as non-compliance at technical evaluation.

| Sl. No | Specification / Requirement | Bidder Compliance Status | Offered Specification / Model | Deviation / Remarks | Supporting Document / Page |
|---|---|---|---|---|---|
| 1 | Enterprise Cyber Range – capacity, virtualization, orchestration, SIEM/XDR and training requirements | | | | |
| 2 | AI/ML Threat Analytics – framework, analytics, telemetry, SIEM/XDR integration and custom AI/ML | | | | |
| 3 | Threat Intelligence Platform – standards, feeds, enrichment, integration and support | | | | |
| 4 | Enterprise Malware Sandbox Appliance – appliance hardware, analysis, integration and 5-year support | | | | |
| 5 | Incident, Case & Digital Evidence Management – lifecycle, evidence, chain of custody and workflow | | | | |
| 6 | Digital Forensic Analysis Suite – | | | | |

| Sl. No | Specification / Requirement | Bidder Compliance Status | Offered Specification / Model | Deviation / Remarks | Supporting Document / Page |
|---|---|---|---|---|---|
| | computer/mobile/memory/network/multimedia forensics and evidence formats | | | | |
| 7 | Cyber Range Training, Research & Capacity Building – exercises, OSINT, research, ToT and knowledge transfer | | | | |
| 8 | Application/Infrastructure Monitoring Dashboard – APM, servers, databases, network, storage, cloud, endpoints and ITSM | | | | |
| 9 | High-Performance Cyber Security Workstation + Command Console – workstation, displays, console, peripherals and 5-year warranty | | | | |

- **Detailed Line-by-Line Compliance Matrix – Bidder Format**

For every parameter under Section 5, the bidder shall reproduce/complete the following matrix. This matrix is intended to become the Technical Bid compliance statement.

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| 1 | Platform | Enterprise Cyber Range supporting ILT, practical labs, CTF, Red/Blue/Purple Team, attack simulation, Incident Response, Malware Analysis, Digital Forensics, SOC training, Cyber Crisis/Tabletop exercises and competency assessments. | | | |
| 1.1 | Capacity | Minimum 200 concurrent trainees, 20 instructors, 300+ VMs, 10+ concurrent labs and 100+ scenarios, with minimum 50% future scalability. | | | |
| 1.2 | Virtualization | VMware vSphere / Hyper-V / Proxmox VE Enterprise / KVM/OpenStack or equivalent with HA, clustering, live migration, templates, snapshots/rollback, | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | monitoring and API integration. | | | |
| 1.3 | Range Management | Centralized web-based orchestration supporting automated VM/network provisioning, isolated environments, lab/scenario deployment, cloning, snapshots, rollback, automated reset, team management and scoring. | | | |
| 1.4 | SIEM/XDR | Enterprise SIEM/XDR using Wazuh with OpenSearch or equivalent, supporting minimum 250 monitored assets, centralized log/event collection, correlation, alerting, threat detection and security analytics. | | | |
| 1.5 | Threat & SOC Analytics | IOC matching, MITRE ATT&CK mapping, UEBA, FIM, vulnerability detection, threat hunting, risk-based alerting, SOC dashboards, reporting, incident/case management and workflow automation. | | | |
| 1.6 | Integration | AD/LDAP, firewalls, IDS/IPS, DNS/DHCP, Suricata, Zeek, MISP, Malware Sandbox, Threat Intelligence, AI/ML Threat Analytics, SAN/NAS, Video Wall, IFMS and other enterprise/security infrastructure through standard interfaces/APIs. | | | |
| 1.7 | Security | RBAC, MFA, SSL/TLS, audit logging, centralized authentication, backup and recovery. | | | |
| 1.8 | Solution Model & Pricing | Proprietary/Commercial, Open-Source or Hybrid. Proprietary and Open-Source options shall be | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | separately priced, including implementation, licenses/subscriptions and 5-year TCO. | | | |
| 1.9 | Training | Minimum 15 working days Administrator Training + 20 working days Instructor Training, including scenario/lab development and Red/Blue/Purple Team, CTF, SOC and Incident Response exercises. | | | |
| 1.9 | Implementation | Complete installation, configuration, customization, integration, testing, performance validation, UAT, commissioning, documentation, SOPs and knowledge transfer. | | | |
| 1.10 | Support | Minimum 5 years comprehensive support, including software/security updates, patches, scenario updates, technical assistance and capacity building. | | | |
| 2 | Platform | Enterprise AI/ML-based Threat Analytics and Security Monitoring Platform, deployed on Department-provided AI/GPU Compute Servers and on-premises Data Centre infrastructure. | | | |
| 2.1 | Architecture | AI/ML analytics layer integrated with the Cyber Range and SIEM/XDR platform; shall not require procurement/deployment of a duplicate SIEM/XDR environment. | | | |
| 2.2 | AI/ML Framework | TensorFlow, PyTorch, Scikit-learn, MLflow, JupyterLab or equivalent enterprise AI/ML | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | frameworks/tools. | | | |
| 2.3 | AI Security Analytics | AI-assisted threat detection, anomaly detection, UEBA, behavioural analytics, predictive threat analytics, threat hunting, malware analytics, IOC correlation, MITRE ATT&CK mapping and risk scoring. | | | |
| 2.4 | Data Sources | Windows, Linux, AD, firewalls, IDS/IPS, DNS, Syslog, NetFlow/IPFIX, Zeek, Suricata, Sysmon, PCAP and Cyber Range exercises. | | | |
| 2.5 | SIEM/XDR Integration | Full integration with Wazuh/OpenSearch or equivalent SIEM/XDR for logs, alerts, IOCs, risk scores and AI-generated threat intelligence. | | | |
| 2.6 | Malware & Threat Intelligence | Integration with Enterprise Malware Sandbox and Threat Intelligence Platform for behavioural analysis, IOC extraction, correlation and threat-intelligence enrichment. | | | |
| 2.7 | Custom AI/ML Development | Development/ customization of AI/ML security use cases, models, detection rules, correlation rules, dashboards, automated reports and threat-hunting workflows. | | | |
| 2.8 | Deployment & APIs | Containerized deployment using Docker or equivalent with REST API/standard interfaces. | | | |
| 2.9 | Security | RBAC, SSL/TLS encryption, audit logging, secure authentication, backup and recovery. | | | |
| 2.9 | Hardware Scope | Department-provided AI/GPU Compute | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | Infrastructure. AI/GPU server hardware is excluded from this BOQ item unless specifically stated otherwise. | | | |
| 2.10 | Implementation & Training | Installation, configuration, customization, integration, testing, UAT, administrator/SOC analyst training, documentation, SOPs, architecture diagrams and knowledge transfer. | | | |
| 2.11 | Support | Minimum 5 years comprehensive software support, including upgrades, security patches, remote/onsite technical assistance and AI/ML solution support. | | | |
| 3 | Platform & Intelligence | Enterprise web-based TIP supporting centralized aggregation, correlation and management of IOCs, TTPs, malware, phishing, ransomware, botnet and vulnerability intelligence, with automated ingestion, enrichment, reputation analysis, threat scoring and campaign tracking. | | | |
| 3.1 | Standards & Integration | STIX/TAXII, OpenIOC, YARA, Sigma, MITRE ATT&CK, CVE/NVD and MISP or equivalent; API integration with Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Malware Sandbox, Suricata, Zeek, Firewalls, EDR/XDR and other security infrastructure. | | | |
| 3.2 | Management, Licensing & Support | IOC search, threat hunting, dashboards, alerts, reporting, intelligence sharing, RBAC, SSL/TLS, | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | audit logging and backup/recovery. Include software licenses, threat-intelligence feeds and connectors, installation, integration, UAT, documentation, training and 5-year comprehensive updates and technical support. | | | |
| 4 | Appliance & Malware Analysis | Dedicated Malware Sandbox Appliance with minimum 16 CPU cores, 64 GB RAM, 2 × 960 GB Enterprise SSD in RAID-1, minimum 4 TB analysis storage and redundant power supplies. Static, dynamic and behavioural analysis, detonation, exploit/ransomware/zero-day detection and AI-assisted threat classification. | | | |
| 4.1 | Threat Analysis & Intelligence | Windows, Linux, Android and macOS-related files/workloads, executables, scripts, PDF/Office documents, archives, email attachments and web downloads; automated IOC extraction, malware reports, MITRE ATT&CK mapping, threat scoring and signature/detection-artifact generation. | | | |
| 4.2 | Integration | SIEM/XDR, NGFW, Threat Intelligence Platform, AI/ML Threat Analytics, Cyber Range, Email Security Gateway, WAF and other security infrastructure, including automated sample submission and verdict/IOC | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | exchange. | | | |
| 4.3 | Management, Licensing & Support | Centralized web management, RBAC, SSL/TLS, audit logging and reporting. Include all hardware, software, licenses, subscriptions, threat-intelligence updates and accessories, installation, integration, testing/UAT, documentation, administrator training and 5-year comprehensive onsite OEM warranty, updates and technical support. | | | |
| 5 | Incident & Case Management | Centralized incident registration, categorization, prioritization, assignment, escalation, investigation, case notes, approvals and complete incident/case lifecycle tracking. | | | |
| 5.1 | Security Response Workflow | Configurable workflows for alert triage, task assignment, escalation, SLA tracking, investigation, containment, remediation, recovery and incident closure. | | | |
| 5.2 | Digital Evidence Management | Centralized registration and management of digital evidence, evidence inventory, evidence assignment, QR/barcode identification, secure evidence attachment/storage and forensic workflow tracking. | | | |
| 5.3 | Evidence Integrity & Chain of Custody | MD5, SHA-256 or stronger hashing, evidence integrity validation, chain-of-custody tracking, version control and complete audit trail. | | | |
| 5.5 | Integration | SIEM/XDR, AI/ML Threat | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | Analytics, Threat Intelligence Platform, Malware Sandbox, Digital Forensic Software/Mobile Forensic Tools, Cyber Range, AD/LDAP and SAN/NAS evidence storage. | | | |
| 5.6 | Dashboard & Reporting | Real-time incident/case/evidence status, severity, response time, SLA compliance, trends, KPIs, evidence tracking, audit trails and management/executive/forensic reports. | | | |
| 5.7 | Security & Access | RBAC, MFA, SSL/TLS, centralized authentication, audit logging, secure API access, backup and recovery. | | | |
| 5.8 | Implementation & Support | Installation/deployment, configuration, customization, integration, testing/UAT, documentation, administrator/user training and 5-year comprehensive software updates, maintenance and technical support. | | | |
| 6 | Forensic Analysis Capability | Computer, Mobile, Memory, Network and Multimedia Forensic Analysis, including file-system analysis, deleted-file recovery, registry, email/browser artefacts, timeline analysis, memory forensics, malware-related artefact analysis and forensic reporting. | | | |
| 6.1 | Evidence Acquisition & Mobile Forensics | Logical, file-system and physical acquisition where technically supported; disk/image acquisition and compatibility with forensic | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | imaging appliances and hardware write-blocking/acquisition kits; Android and iOS mobile forensic acquisition/analysis where supported. | | | |
| 6.2 | Image & Video Forensics | Enhancement, deblurring, frame-level analysis, authentication/integrity examination, object tracking, metadata extraction and relevant multimedia forensic analysis. | | | |
| 6.3 | Evidence Formats & Platforms | Windows, Linux, macOS, Android and iOS; RAW/DD, E01/Ex01, AFF/AFF4, VMDK, VHD/VHDX or equivalent. | | | |
| 6.4 | Evidence Integrity & Case Management | MD5, SHA-1, SHA-256 or stronger hashing, evidence verification, bookmarking/tagging, chain-of-custody, case management, investigation notes, audit trails and customizable forensic reports. | | | |
| 6.5 | Enterprise Integration | SIEM/XDR, Incident & Case Management, Threat Intelligence Platform, Malware Sandbox, Cyber Range and SAN/NAS evidence storage through APIs, IOC/file exchange or equivalent. | | | |
| 6.6 | Licensing, Security & Support | Appropriate multi-user/concurrent licensing, centralized license/user management and RBAC; all software/licenses, installation, configuration, integration, testing/UAT, training, documentation | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | and 5-year comprehensive updates/upgrades/support. | | | |
| 7 | Cyber Range Scenarios & Exercises | Cyber Range simulations, Red Team, Blue Team, Purple Team, CTF, Tabletop, Cyber Crisis, SOC, Incident Response, Digital Forensics, Malware Analysis and Threat Hunting exercises. | | | |
| **7.1** | Training & Capacity Building | Instructor-led and hands-on training covering Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Incident/Evidence Management, Digital/Mobile Forensics, Blockchain Investigation, servers, storage, virtualization, networks, firewall and associated ICT/security solutions. | | | |
| **7.2** | Research & Analysis Tools | Cybersecurity research, OSINT, threat research, data correlation, link/relationship analysis, timeline and graph analysis, visualization, dashboards and intelligence analysis, with AI/ML-assisted analytics where applicable. | | | |
| **7.3** | Integration | Integration with Cyber Range, SIEM/XDR, Threat Intelligence, Digital Forensics, Incident & Evidence Management and other project platforms through APIs/interfaces. | | | |
| **7.4** | Training Content & Knowledge Transfer | Training manuals, SOPs, administrator/user guides, laboratory exercises, scenarios, presentations, case studies, assessments | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | and Train-the-Trainer (ToT), including refresher/advanced training during support period. | | | |
| **7.5** | Implementation Model & Support | Training/scenarios and research tools shall be provided module-wise and as required by the Department; licensing, customization, configuration, updates and technical support shall be included. | | | |
| 8 | Platform | Enterprise web-based Application & Infrastructure Monitoring Dashboard Platform with centralized administration and management. | | | |
| 8.1 | Monitoring Capability | Centralized monitoring of applications/APM, servers, databases, networks, storage, virtualization, cloud infrastructure and endpoints. | | | |
| 8.2 | Dashboard & Analytics | Real-time interactive dashboards, customizable widgets, KPI monitoring, reports, analytics, alerts, notifications, historical data and trend analysis. | | | |
| 8.3 | Infrastructure Integration | Windows, Linux, VMware/Hyper-V, Docker/containers, databases, storage, network/security devices, SNMP, Syslog, WMI and REST APIs. | | | |
| 8.4 | Enterprise Integration | AD/LDAP, Cyber Range, SIEM/XDR, SAN/NAS, servers, network infrastructure and departmental applications/platforms. | | | |
| 8.5 | IT Operations & | Workflow automation, asset inventory, | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | Automation | configuration management, SLA monitoring, helpdesk/ticketing integration and ITSM capabilities. | | | |
| 8.6 | Alerts & Reporting | Threshold/event alerts, scheduled reports, email/SMS or equivalent notifications, performance analysis and capacity/trend reporting. | | | |
| 8.7 | Security | RBAC, centralized authentication, SSL/TLS encryption, audit logging and backup/restore. | | | |
| 8.8 | Solution Model | Zoho/ManageEngine or equivalent enterprise platform meeting/exceeding the specified requirements. | | | |
| 8.9 | Licensing | All required licenses/subscriptions, connectors, monitoring agents, APIs and management components. | | | |
| 8.10 | Implementation | Supply, installation, configuration, customization, integration, testing, UAT and commissioning. | | | |
| 8.11 | Documentation & Training | Architecture/configuration documentation, SOPs, administrator training, user training and knowledge transfer. | | | |
| 8.12 | Support | Minimum 5 years comprehensive software support including updates, upgrades, security patches and technical assistance. | | | |
| 9 | Type | Enterprise high-performance workstation with integrated ergonomic command/operator console suitable for SOC, Cyber Range, Red/Blue/Purple | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| | | Team and advanced cyber-security operations. | | | |
| 9.1 | Processor | Intel Core i9 current/latest generation or equivalent/better. | | | |
| 9.2 | Memory | Minimum 64GB DDR5 RAM, expandable to minimum 128 GB or higher. | | | |
| 9.3 | Storage | Minimum 2 TB PCIe Gen4 NVMe SSD with provision for additional internal storage. | | | |
| 9.4 | Graphics | Professional-grade dedicated GPU with adequate compute performance and memory capacity to support Cyber Security, SOC, Cyber Range, security analytics and multiple high-resolution display workloads. | | | |
| 9.5 | Displays | Dual 27-inch or higher IPS/QHD displays, anti-glare, with suitable dual-monitor mounting. | | | |
| 9.6 | Networking | Minimum 2.5 GbE Ethernet, Wi-Fi 6E or better and Bluetooth. | | | |
| 9.7 | Operating System | Windows 11 Pro 64-bit or equivalent professional OS, with Linux/virtualization support. | | | |
| 9.8 | Software Compatibility | Cyber Range, virtualization, SIEM/XDR, SOC monitoring, packet/network analysis, threat intelligence, security analysis and remote administration tools. | | | |
| 9.9 | Security | TPM 2.0, Secure Boot, BIOS/UEFI security, BitLocker/drive encryption support, endpoint protection and centralized management. | | | |

| Section | Parameter | Tender Requirement | Compliance Status (YES/NO/PARTIAL) | Bidder's Offered Specification / Deviation | Document / Page Ref. |
|---|---|---|---|---|---|
| 9.10 | Integration | Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Video Wall, AD/LDAP and centralized authentication. | | | |
| 9.11 | Command Console | Professional ergonomic operator/command console with dual-monitor mounts, concealed cable management, power/data provisions and equipment/storage space. | | | |
| 9.12 | Peripherals | Professional keyboard/mouse, USB headset with microphone, Full-HD or better webcam and all necessary cables/adapters/accessories. | | | |
| 9.13 | Installation | Complete supply, installation, configuration, integration, testing and commissioning. | | | |
| 9.14 | Warranty | Minimum 5-year comprehensive onsite OEM warranty and technical support. | | | |

- **Eligibility Criteria**

| Sl. No | Eligibility Criterion | Supporting Document |
|---|---|---|
| 1 | Bidder must be registered in India and have been in operations for minimum 3 years as on bid opening. | GST Registration Certificate and PAN or COI |
| 2 | Average annual turnover of at least ₹10 Crores from IT Infrastructure business during last 3 financial years. | Audited financial statements for last 3 FYs |
| 3 | Bidder must not have been blacklisted, debarred or suspended by any Central/State Government or PSU during last 3 years. | Undertaking on company letterhead signed by Authorized Signatory |
| 4 | Positive net worth for each of last 3 financial years. | Audited Balance Sheet and/or CA Certificate |
| 5 | Bidder must be authorized reseller/partner for all quoted products and solutions. | Manufacturer Authorization Form specific to this tender |
| 6 | OEM from a country sharing land border with India | Supporting registration |

| Sl. No | Eligibility Criterion | Supporting Document |
|---|---|---|
| | eligible only if registered with competent authority as per applicable Government of India order. | documents |
| 7 | OEM undertaking that offered items are not nearing end-of-life/end-of-support until end of warranty. | Supporting undertaking/document |
| 8 | Project Experience: The bidder shall have successfully executed similar Enterprise Cyber Security Software projects during the last five (5) years and shall meet any one of the prescribed experience routes. Experience in Cyber Range/Cyber Training Platforms, SIEM/XDR, Threat Intelligence, AI/ML-based Cyber Security Analytics, Malware Analysis, Digital Forensics, Incident/Case/Digital Evidence Management, Cyber Security Research Platforms, or integration/customization of Enterprise Cyber Security Software solutions shall be considered relevant. Experience in any one or more of these categories shall be sufficient and the bidder shall not be required to demonstrate experience in all categories. | PO copies and completion reports |
| 9 | Mandatory pre-bid participation and site visit; written consent after pre-bid and Site Visit Certificate with Technical Bid. | Pre-bid/site visit documents and certificate |

- **Pre-Bid Meeting**

Participation in the pre-bid discussion is compulsory/mandatory through offline/online mode. Offers/bids of service providers who do not participate may not be considered for further evaluation, as stated in the source tender.

After attending the pre-bid discussion, the service provider shall submit written consent confirming understanding of the terms and quantum of work.

- **Commercial Conditions & Payment Terms**

Bids shall be submitted online through the Kerala e-GP system. Two covers are prescribed: (i) Technical Bid and (ii) Financial Bid. Foreign equipment rates shall be quoted in Indian Rupees.

| Source Payment Provision | Draft Status |
|---|---|
| Payment Clause | Payment will be released only after successful completion of supply, installation, configuration and commissioning of the project.<br>Request for advance payment, if any, will be considered as per rules, on request from the supplier and against submission of a valid Bank Guarantee. |

- **Other Payment Terms**

1. PBG shall be in favour of the Director General of Police, Kerala State.
2. PBG shall remain valid for contract period + 3 months.
3. Advance shall be adjusted in subsequent bills.
4. No advance without Bank Guarantee as per KFC Rule 182A & KSPM Clause 15.15.

- **General Conditions**

- ✓ Department reserves the right to accept or reject any/all bids, in full or in part, without assigning a reason. Contract may be awarded to the lowest evaluated bidder or a technically qualified firm whose proposal is considered most advantageous.
- ✓ Strict confidentiality of all departmental data, systems and information shall be maintained.
- ✓ No departmental data or information shall be copied, transferred or exported outside India under any circumstances.
- ✓ Selected firm shall commence work immediately upon issue of Work Order and signing of Agreement.
- ✓ Subcontracting is permitted only with prior written approval of the Department.
- ✓ Penalties/liquidated damages shall apply for delays, non-performance or breach as per rules.
- ✓ Bidders may propose equivalent or superior items, subject to technical evaluation and Department approval.
- ✓ Department decision on bid evaluation, award and execution shall be final and binding.
- ✓ OEM/Solution Provider shall submit duly filled compliance statement as prescribed. Non-submission may lead to rejection.
- ✓ Quoted items shall not be declared End of Sale for the next five years from bid submission.

- **Mode of Submission and e-Tender Conditions**

1. Online submission only through the Kerala e-GP website.
2. Two covers: Technical Bid and Financial Bid.
3. Foreign equipment rates shall be quoted in Indian Rupees.
4. Tender documents shall be downloaded only during the notified period.
5. Digitally signed tender and specified documents shall be uploaded before the last date/time.
6. Tender fee shall be paid online; non-payment may result in outright rejection.
7. EMD shall be paid online. Eligible SPD Kerala/National Small Scale Industries Corporation registered bidders may claim exemption with valid documentary proof.
8. Withdrawal and re-submission are permitted only until the last date/time for submission.
9. Bids shall be opened online at the Office of State Police Chief, Police Headquarters, Thiruvananthapuram.
10. Financial bids of technically qualified tenderers only shall be considered for opening.
11. All tenderers quoting the items shall be ready for technical evaluation at Thiruvananthapuram on the date intimated by the Department.
12. Hard copies of relevant tender documents shall be produced at technical evaluation when required.

13. Uploaded documents shall bear signature/office seal of bidder/authorized person and shall be digitally signed.
14. Bidders shall ensure compliance with Digital Signature Certificate requirements and e-GP procedures.

- **Testing, Documentation, Commissioning & Knowledge Transfer**

15. Installation testing
16. Configuration validation
17. Functional testing
18. Integration testing
19. Security validation
20. Performance testing
21. User Acceptance Testing (UAT)
22. Final commissioning
23. System Architecture Documentation
24. Configuration Documents
25. Administrator Manuals
26. User Manuals
27. Standard Operating Procedures (SOPs)
28. API Documentation
29. License Documentation
30. Test Reports
31. Commissioning Reports
32. As-built Documentation
33. Training manuals, hands-on sessions and knowledge transfer documentation

- **Training & Knowledge Transfer**

34. Platform Administration
35. User Administration
36. Security Operations
37. Threat Detection & Investigation
38. Malware Analysis
39. Incident Management
40. Digital Forensic Operations
41. Reporting & Dashboard Management
42. Backup & Recovery
43. Preventive Maintenance
44. Basic Troubleshooting
45. Administrator and user training
46. Hands-on sessions, manuals, guides and knowledge transfer

- **Warranty, Support & Maintenance**

47. All applicable software licenses, subscriptions and activation keys shall be supplied.
48. Five (5) years comprehensive OEM/software support or as specified in the BOQ.
49. Software updates, security patches and version upgrades during the support period.
50. Remote and onsite technical support, as applicable.

51. Bug fixes, troubleshooting and incident resolution.
52. Coordination with OEMs for issue resolution.
53. Maintenance of the complete integrated software environment throughout the contract period.
54. Module-specific support requirements in the technical specifications shall also apply.

- **Bidder Compliance Declaration**

We hereby certify that the information and technical compliance statements submitted with this bid are true and complete. All deviations, limitations, dependencies, licensing restrictions and assumptions have been explicitly disclosed.

| Declaration | Bidder Entry |
|---|---|
| Bidder Name | |
| Authorized Signatory | |
| Designation | |
| Date | |
| Place | |
| Company Seal | |
| Overall Technical Compliance | COMPLIED / PARTIALLY COMPLIED / NOT COMPLIED |
| Commercial Compliance | COMPLIED / DEVIATION |
| Deviation Schedule Attached | YES / NO |

- **Deviation / Exception Schedule**

Any deviation from a minimum requirement must be listed here. If there are no deviations, the bidder shall write 'NIL'.

| Sl. | Tender Section / Clause | Tender Requirement | Bidder's Deviation / Exception | Impact | Department Decision |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |

- **Compliance Status Legend**

| Status | Meaning |
|---|---|
| COMPLIED | Bidder fully meets or exceeds the stated minimum requirement. |
| PARTIALLY COMPLIED | Bidder meets part of the requirement but has a stated limitation or gap. |
| NOT COMPLIED | Bidder does not meet the requirement. |
| DEVIATION | Bidder proposes an alternative or departure requiring Department evaluation/approval. |
| NOT APPLICABLE | Requirement genuinely does not apply; bidder must provide justification. |

- **Overall Responsibility of the Selected Bidder**

The selected bidder shall be responsible for the complete end-to-end delivery, implementation and operationalization of the proposed Enterprise Cyber Security Software Solution(s), covering one or more of the specified solution areas, including:

- ✓ Supply / licensing of proprietary software or provision of open-source software components, as applicable.
- ✓ Installation, configuration and customization of the proposed software solutions.
- ✓ Integration and interoperability with the existing and proposed Cyber Operations infrastructure and other relevant departmental systems.
- ✓ Development and implementation of required APIs, connectors, interfaces, workflows, dashboards and reports.
- ✓ Testing, security validation, User Acceptance Testing (UAT), commissioning and performance validation.
- ✓ Provision of all required implementation tools, middleware, connectors, documentation and technical components necessary for successful deployment.
- ✓ Administrator training, user training, Train-the-Trainer (ToT) and knowledge transfer.
- ✓ Preparation and submission of system architecture, configuration documents, user manuals, administrator manuals and SOPs.
- ✓ Provision of applicable software updates, upgrades, security patches, bug fixes and technical support during the contract/support period.
- ✓ Provision of warranty and comprehensive support and maintenance as specified in the RFP.

The bidder shall ensure that all proposed software components are fully functional, interoperable, secure, scalable and operational upon completion of the implementation. All necessary licenses, subscriptions, APIs, connectors, customization, integration services, documentation, training and other associated requirements shall be clearly identified and quoted in the Commercial Bid/BOQ, wherever applicable. **The entire project cost should be quoted in the BOQ as a whole.**

- **Contact for Clarifications**

  Cyber Operations Wing, Kerala Police

  Email: cyberops-sec.pol@kerala.gov.in

  Clarifications should be submitted well in advance of the bid submission deadline.

  Source contact / technical clarification reference: Assistant Sub Inspector of Police, Cyber Security and Advanced Crimes, Cyber Operations, PHQ, telephone 9895258496.

- **General Conditions**

1. Right of the Department: The Department reserves the right to accept or reject any or all bids, in whole or in part, and to modify or cancel the tender process in accordance with applicable Government rules.
2. Quantity/Scope Variation: The Department may increase, decrease, omit or combine items/quantities within the approved budget and as permitted under applicable procurement rules.
3. Confidentiality: The bidder shall maintain strict confidentiality of all departmental data, systems, documents, credentials and information.

4. Data Residency: Departmental data and information shall remain within India and shall not be transferred or stored outside India without prior written approval of the Department and as permitted by applicable rules.
5. Commencement: The successful bidder shall commence work within the period specified in the Work Order/Agreement.
6. Subcontracting: Subcontracting shall be permitted only with prior written approval of the Department. The bidder shall remain fully responsible for the contracted work.
7. Penalty/LD: Liquidated damages, penalties or other contractual remedies shall apply for delay, non-performance or breach as specified in the RFP/SLA.
8. Equivalent Solutions: Bidders may offer equivalent or higher-performing products/solutions meeting the prescribed minimum requirements, subject to technical evaluation and approval.
9. Technical Compliance: A duly completed and digitally signed Technical Compliance Statement shall be submitted in the prescribed format. Non-submission may result in rejection.
10. Product Lifecycle: Offered proprietary products/solutions shall not be End-of-Sale/End-of-Life at the time of bidding and shall have OEM support, updates and security patches for the required contract period.
11. Online Submission: All bids shall be submitted online only through the Kerala e-GP portal in the prescribed covers. No other mode of submission shall be accepted.
12. Bid Covers: The e-Tender shall be submitted in two covers – Technical Bid and Financial Bid, as specified in the e-GP portal.
13. Tender Fee & EMD: Tender fee and EMD, wherever applicable, shall be remitted online through the e-GP portal. Valid exemptions shall be supported by required documents.
14. Withdrawal/Resubmission: Bids may be withdrawn or resubmitted through the e-GP portal up to the prescribed closing date and time.
15. Bid Opening: Bids shall be opened electronically through the e-GP portal on the date and time specified in the tender. Only technically qualified bidders shall proceed to financial evaluation.
16. Technical Evaluation: The Technical Evaluation Committee may evaluate compliance, experience, OEM documentation, demonstrations/PoC, technical presentations and other requirements specified in the RFP.
17. Document Verification: The Department may require original/certified copies of uploaded documents for verification.
18. Clarifications: Bidders shall seek clarifications through the prescribed e-GP mechanism within the specified period. Only official clarifications/corrigenda issued by the Department shall be binding.
19. Digital Signature: Bidders shall possess a valid Digital Signature Certificate (DSC) and digitally sign documents as required by the e-GP system.
20. SLA: The successful bidder shall execute the prescribed Service Level Agreement (SLA) covering support, response/resolution times, escalation, availability and applicable penalties.
21. Decision of Department: Decisions of the Department/competent authority shall be governed by the tender conditions and applicable Government procurement rules.
22. The selected firm shall complete the delivery, installation, configuration and commissioning of all items listed in the annexures within **Ninety Days (90) days** from the date of issue of Work Order/Supply Order.

- **Note to Bidders:-**

1. Bidders have to procure legally valid Digital Certificate (Class III) as per Information

Technology Act, 2000 for digitally signing their electronic bids. Bidders can procure the same from any of the license certifying authority of India. For more details, please visit the e-GP website www.etenders.kerala.gov.in

2. Bidders are advised to note the Tender Id and Tender No. & Date for future reference.

3. All uploaded documents should contain the signature and the office seal of the bidder/authorized persons and should be digitally signed while uploading. Documents uploaded without digitally signing shall entitle rejection of the tender.

4. In the case of Foreign Equipment, the rate should be quoted in Indian Rupees. Preference will be given to those who are ready to supply the item without opening Letter of Credit. Ordinarily, no advance payment will be made for procuring the above item.

v). For obtaining Digital Signature Certificate and help on etendering process, contact Kerala State IT Mission, eGovernment Procurement PMU & Help desk, Basement floor of Pension Treasury Building, Uppalam Road, Statue, Thiruvananthapuram; Ph :0471-2577088, 2577 IBB; Toll free no: 18002337315; e- mail:etendershelo@kerala.gov. in; Website: www.etenders.kerala.gov.in on all government working days from 9:30 am to 5:30 pm.

vi). Successful bidder should execute a service level agreement format available at the Office of IGP Cyber Operations, Pattom Thiruvananthapuram. Cost of stamp paper for SLA is one rupee for every rupee 1000 or part thereof on the amount agreed in the contract, subject to a minimum of rupees 200 and a maximum of rupees one lakh.

Vii)**. Contact for Clarifications**

**For any clarifications regarding this tender, bidders may contact the Cyber Operations Wing, Kerala Police:**

- **Email:** "cyberops-sec.pol@kerala.gov.in"

All queries should be sent well in advance of the bid submission deadline to ensure a response in time.

**NOTE:-BIDDERS ARE ADVISED TO GO THROUGH THE CONDITIONS IN THE NOTICE INVITING TENDER AND THE TENDER DOCUMENT CAREFULLY AND COMPLY WITH THEM TO AVOIDOUTRIGHT REJECTION OF THEIR TENDER.**

**Bidders are requested to make online payment of EMD and tender fee before 72 hours in advance of last date.**

For any litigation relating to this order, the jurisdiction will be Thiruvananthapuram City.

Sd/-
Assistant Inspector General of Police, Procurement
For DIRECTOR GENERAL OF POLICE &
STATE POLICE CHIEF, KERALA

# eTendering System Government of Kerala

## Tender Details

Date : 15-Sep-2026 02:52 PM

Print

### Basic Details

| | | | |
|---|---|---|---|
| **Organisation Chain** | Kerala Police\|\|Police Headquarters | | |
| **Tender Reference Number** | KPET/39/2026/PHQ | | |
| **Tender ID** | 2026_KP_870062_1 | **Withdrawal Allowed** | Yes |
| **Tender Type** | Open Tender | **Form of contract** | Item Wise |
| **Tender Category** | Goods | **No. of Covers** | 2 |
| **General Technical Evaluation Allowed** | No | **ItemWise Technical Evaluation Allowed** | No |
| **Payment Mode** | Online | **Is Multi Currency Allowed For BOQ** | No |
| **Is Multi Currency Allowed For Fee** | No | **Allow Two Stage Bidding** | No |

### Payment Instruments

**Online Bankers**

| S.No | Bank Name |
|---|---|
| 1 | SBI MOPS |

### Cover Details, No. Of Covers - 2

| Cover No | Cover | Document Type | Description |
|---|---|---|---|
| 1 | Fee/PreQual/Technical | .pdf | Scanned copy of agreement executed on Kerala Stamp paper Rs. 200 duly signed and sealed in all pages |
| | | .pdf | Scanned copy of Tender Document duly signed and sealed in all pages |
| | | .pdf | Brochures or diagrams of the tems quoted in the bid |
| | | .pdf | Copies of other documents required in the Notice Inviting Tender and scope of work |
| | | .pdf | Any other documents or conditions of suppy if any |
| 2 | Finance | .xls | Financial Bid |
| | | .pdf | Itemwise price details of bill of materials in the Notice Inviting Tender |

## Other Important Documents

| S.No | Category | Sub Category | Sub Category Description | Format/File |
|---|---|---|---|---|
| 1 | Certificate Details | Permanent Account Number | Permanent Account Number | |
| 2 | Certificate Details | Registration Certificate | Registration Certificate | |
| 3 | Certificate Details | Income Tax Certificate | Income Tax Certificate | |
| 4 | Certificate Details | Partnership Deed | Partnership Deed | |
| 5 | Certificate Details | Labour License | Labour License | |
| 6 | Certificate Details | Power of Attorney | Power of Attorney | |
| 7 | Certificate Details | Affidavit regarding correctness of bid | Required in tender document in bidder file 1 | |
| 8 | Certificate Details | Excise registration Number | Excise registration Number | |
| 9 | Certificate Details | Service tax registration No | Service tax registration No | |
| 10 | Certificate Details | GST Certificate | GST Certificate | |
| 11 | Financial Details | Bankers Details | Bankers Details | |
| 12 | Financial Details | Annual Turn over certificates from CA | Annual Turn over certificates from CA | |
| 13 | Financial Details | B23. P/L and Balance Sheet 2022-2023 | P/L and Balance Sheet 2022-2023 | |
| 14 | Financial Details | B24 P/L and Balance Sheet 2023-2024 | P/L and Balance Sheet 2023-2024 | |
| 15 | Financial Details | B25. P/L and Balance Sheet 2024-2025 | P/L and Balance Sheet 2024-2025 | |
| 16 | Miscellaneous | Work Completed Certificate Copies | Work Completed Certificate Copies | |
| 17 | Miscellaneous | Company profile | Company profile | |
| 18 | Work Details | Works Completed Details | Works Completed Details | |
| 19 | Work Details | Quantity of Work Done Details | Quantity of Work Done Details | |

## Tender Fee Details, [Total Fee in ₹ * - 30,284]

| | | | |
|---|---|---|---|
| **Tender Fee in ₹** | 28,750 | | |
| **Processing Fee in ₹ (18.00% GST Incl.)** | 1,534 | | |
| **Fee Payable To** | Nil | **Fee Payable At** | Nil |
| **Tender Fee Exemption Allowed** | Yes | | |

## EMD Fee Details

| | | | |
|---|---|---|---|
| **EMD Amount in ₹** | 3,71,000 | **EMD Exemption Allowed** | Yes |
| **EMD Fee Type** | fixed | **EMD Percentage** | NA |
| **EMD Payable To** | Nil | **EMD Payable At** | Nil |

Click to view modification history

## Work /Item(s)

| | | | | | |
|---|---|---|---|---|---|
| **Title** | Establishment of Integrated Cyber Security Software and Simulation Platforms with Supporting Hardware Infrastructure at the Police Training College, Thiruvananthapuram | | | | |
| **Work Description** | Establishment of Integrated Cyber Security Software and Simulation Platforms with Supporting Hardware Infrastructure at the Police Training College, Thiruvananthapuram | | | | |
| **Pre Qualification Details** | Refer Notice Inviting Tender and specification | | | | |
| **Independent External Monitor/Remarks** | NA | | | | |
| **Show Tender Value in Public Domain** | Yes | | | | |
| **Tender Value in ₹** | 3,71,00,000 | **Product Category** | Equipments | **Sub category** | Integrated Cyber Security Software |
| **Contract Type** | Tender | **Bid Validity(Days)** | 180 | **Period Of Work(Days)** | 90 |

| | | | | | |
|---|---|---|---|---|---|
| **Location** | Thriuvananthapuram | **Pincode** | 695010 | **Pre Bid Meeting Place** | NA |
| **Pre Bid Meeting Address** | NA | **Pre Bid Meeting Date** | NA | **Bid Opening Place** | Police Headquarters Thiruvananthapuram |
| **Should Allow NDA Tender** | No | **Allow Preferential Bidder** | No | | |
| **Tenderer Class** | Not Applicable | | | | |

## Critical Dates

| | | | |
|---|---|---|---|
| **Publish Date** | 15-Sep-2026 05:00 PM | **Bid Opening Date** | 29-Sep-2026 03:00 PM |
| **Document Download / Sale Start Date** | 15-Sep-2026 05:00 PM | **Document Download / Sale End Date** | 28-Sep-2026 12:00 PM |
| **Clarification Start Date** | NA | **Clarification End Date** | NA |
| **Bid Submission Start Date** | 15-Sep-2026 05:00 PM | **Bid Submission End Date** | 28-Sep-2026 12:00 PM |

## Tender Documents

**NIT Document**

| S.No | Document Name | Description | Document Size (in KB) |
|---|---|---|---|
| 1 | Tendernotice_1.pdf | Notice Inviting Tender and specification | 479.10 |

**Work Item Documents**

| S.No | Document Type | Document Name | Description | Document Size (in KB) |
|---|---|---|---|---|
| 1 | Other Document | ScopeofWork.pdf | Scope of Work | 447.71 |
| 2 | BOQ | BOQ_1474181.xls | Financial Bid | 57.00 |
| 3 | Tender Documents | Generalconditions.pdf | Tender Document, General conditions, format for agreement etc | 273.00 |

## Bid Openers List

| S.No | Bid Opener Login Id | Bid Opener Name | Certificate Name |
|---|---|---|---|
| 1. | sekharpramod@gmail.com | PRAMOD S | PRAMOD S |
| 2. | sastha@gmail.com | SASTHA RAJ R | SASTHA RAJ R |
| 3. | shibikshibi0@gmail.com | SHIBI K | SHIBI K |

## Tender Properties

| | | | |
|---|---|---|---|
| **Auto Tendering Process allowed** | No | **Show Technical bid status** | Yes |
| **Show Finance bid status** | Yes | **Stage to disclose Bid Details in Public Domain** | Technical Bid Opening |
| **BoQ Comparative Chart model** | Normal | **BoQ Compartive chart decimal places** | 2 |
| **BoQ Comparative Chart Rank Type** | H | **Form Based BoQ** | No |

## Tender Inviting Authority

| | |
|---|---|
| **Name** | DGP and State Police Chief Keralam |
| **Address** | Police Headquarters Vazhuthacaud Thiruvananthapuram Keralam |

## Tender Creator Details

| | |
|---|---|
| **Created By** | SHIBI K |
| **Designation** | Senior Superintendent |
| **Created Date** | 15-Sep-2026 02:24 PM |