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

Proposed location: 2nd Floor, Police Training College, under the Scheme of ASUMP 2026-2027.

Complete end-to-end supply, licensing, installation, configuration, customization, integration, testing, commissioning, documentation, training, knowledge transfer, warranty and comprehensive technical support.

All software components, licenses, subscriptions, APIs, connectors, implementation tools, documentation, training materials and other items necessary for a fully functional integrated solution shall be included whether or not individually identified in the BOQ.

The solution shall be modular and scalable. Individual modules shall be capable of independent or collective implementation and commissioning while maintaining interoperability with the overall Cyber Range and Cyber Security ecosystem.

Bidder may propose proprietary/commercial, customized open-source or hybrid solutions meeting or exceeding the stated functional, security, integration, performance and support requirements.

The bidder shall clearly identify solution model, components, licensing/subscription requirements and associated costs in the technical and commercial proposal.

1. 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	Enterprise Cryptocurrency & Blockchain Analytics / Digital Asset Investigation Platform	Blockchain tracing, wallet analytics, transaction graph and digital asset intelligence
8	Cyber Range Scenarios, Cyber Security Training, Research, Capacity Building & Advanced Analysis	Training, exercises, research tools, OSINT, analysis and knowledge transfer
9	Enterprise Application, Infrastructure & IT Operations Monitoring Dashboard Platform	APM, servers, databases, networks, storage, virtualization, cloud, endpoints and ITSM
10	Enterprise High-Performance Cyber Security Workstation with Integrated Command Console	SOC/Cyber Range operator workstation, dual displays, console and peripherals

2. 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 / 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,

Parameter	Minimum Technical Requirement
	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 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.

Parameter	Minimum Technical Requirement
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,

Parameter	Minimum Technical Requirement
	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 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.

Parameter	Minimum Technical Requirement
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.
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.

Parameter	Minimum Technical Requirement
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

Parameter	**Minimum Technical Requirement**
Type	Enterprise high-performance workstation with integrated ergonomic command/operator console suitable for SOC, Cyber Range, Red/Blue/Purple Team and advanced cyber-security operations.
Processor	Intel Core i9 current/latest generation or AMD Ryzen 9 equivalent/better.
Memory	Minimum 32 GB DDR5 RAM, expandable to minimum 64 GB or higher.
Storage	Minimum 2 TB PCIe Gen4 NVMe SSD with provision for additional internal storage.
Graphics	Dedicated GPU with minimum 8 GB GDDR6 VRAM or better, supporting multiple high-resolution displays.
Displays	Dual 27-inch or higher IPS/QHD displays, anti-glare, with suitable dual-monitor mounting.
Networking	Minimum 1/2.5 GbE Ethernet, Wi-Fi 6E or better and Bluetooth.
Operating System	Windows 11 Pro 64-bit or equivalent professional OS, with Linux/virtualization support.
Software Compatibility	Cyber Range, virtualization, SIEM/XDR, SOC monitoring, packet/network analysis, threat intelligence, security analysis and remote administration tools.
Security	TPM 2.0, Secure Boot, BIOS/UEFI security, BitLocker/drive encryption support, endpoint protection and centralized management.
Integration	Cyber Range, SIEM/XDR, AI/ML Threat Analytics, Threat Intelligence, Malware Sandbox, Video Wall, AD/LDAP and centralized authentication.
Command Console	Professional ergonomic operator/command console with dual-monitor mounts, concealed cable management, power/data provisions and equipment/storage space.
Seating	Heavy-duty high-back ergonomic operator chair with adjustable height, lumbar support and armrests.

Parameter	Minimum Technical Requirement
Peripherals	Professional keyboard/mouse, USB headset with microphone, Full-HD or better webcam and all necessary cables/adapters/accessories.
Installation	Complete supply, installation, configuration, integration, testing and commissioning.
Warranty	Minimum 5-year comprehensive onsite OEM warranty and technical support.

3. 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 – 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 –				

Sl. No	Specification / Requirement	Bidder Compliance Status	Offered Specification / Model	Deviation / Remarks	Supporting Document / Page
	workstation, displays, console, peripherals and 5-year warranty				

4. 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, 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.			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
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 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.			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
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 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,			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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 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			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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, 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,			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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 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			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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 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,			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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 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,			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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 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,			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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 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	Centralized monitoring of			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
	Capability	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 & Automation	Workflow automation, asset inventory, 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			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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 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	Dedicated GPU with minimum 8 GB GDDR6 VRAM or better, supporting multiple high-resolution displays.			
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,			

Section	Parameter	Tender Requirement	Compliance Status (YES/NO/PARTIAL)	Bidder's Offered Specification / Deviation	Document / Page Ref.
		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.			
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.			

5. 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 eligible only if registered with competent authority as per applicable Government of India order.	Supporting registration 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

6. Pre-Bid Meeting & Site Visit

Participation in the pre-bid discussion is compulsory/mandatory through offline 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.

Personnel details and ID proof details for the pre-bid meeting shall be communicated to the specified Cyber Operations email quoting the tender number, on or before the date prescribed in the tender notice. The bidder shall visit the site before bid submission and obtain a Site Visit Certificate, which shall be submitted with the Technical Bid.

Source date retained: **28.08.2026** for the pre-bid participant details email deadline.

Department shall confirm/update this date before issue.

7. 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.

Stage	Source Payment Provision	Draft Status
A	45% advance against Bank Guarantee.	Retained from source; Department to confirm.
B	25% of contract value after confirmation of shipment and acceptance by Kerala Police of each item. Source text parenthetically says 'Seventy Five Percent'.	Arithmetic/wording inconsistency in source; Department to confirm intended percentage.
C	20% after satisfactory installation, testing & commissioning and successful installation report.	Retained from source.
D	Balance 5% against submission of Bank Guarantee from a Nationalized/Scheduled Bank.	Retained from source.

8. Other Payment Terms

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

9. General Conditions

1. 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.
2. Strict confidentiality of all departmental data, systems and information shall be maintained.
3. No departmental data or information shall be copied, transferred or exported outside India under any circumstances.
4. Selected firm shall commence work immediately upon issue of Work Order and signing of Agreement.
5. Subcontracting is permitted only with prior written approval of the Department.
6. Penalties/liquidated damages shall apply for delays, non-performance or breach as per rules.
7. Bidders may propose equivalent or superior items, subject to technical evaluation and Department approval.
8. Department decision on bid evaluation, award and execution shall be final and binding.
9. OEM/Solution Provider shall submit duly filled compliance statement as prescribed. Non-submission may lead to rejection.
10. Quoted items shall not be declared End of Sale for the next five years from bid submission.

10. Mode of Submission and e-Tender Conditions

- ✓ Online submission only through the Kerala e-GP website.
- ✓ Two covers: Technical Bid and Financial Bid.
- ✓ Foreign equipment rates shall be quoted in Indian Rupees.
- ✓ Tender documents shall be downloaded only during the notified period.
- ✓ Digitally signed tender and specified documents shall be uploaded before the last date/time.
- ✓ Tender fee shall be paid online; non-payment may result in outright rejection.
- ✓ EMD shall be paid online. Eligible SPD Kerala/National Small Scale Industries Corporation registered bidders may claim exemption with valid documentary proof.
- ✓ Withdrawal and re-submission are permitted only until the last date/time for submission.
- ✓ Bids shall be opened online at the Office of State Police Chief, Police Headquarters, Thiruvananthapuram.
- ✓ Financial bids of technically qualified tenderers only shall be considered for opening.
- ✓ All tenderers quoting the items shall be ready for technical evaluation at Thiruvananthapuram on the date intimated by the Department.
- ✓ Hard copies of relevant tender documents shall be produced at technical evaluation when required.
- ✓ Uploaded documents shall bear signature/office seal of bidder/authorized person and shall be digitally signed.
- ✓ Bidders shall ensure compliance with Digital Signature Certificate requirements and e-GP procedures.

11. Testing, Documentation, Commissioning & Knowledge Transfer

- ✓ Installation testing
- ✓ Configuration validation
- ✓ Functional testing
- ✓ Integration testing
- ✓ Security validation
- ✓ Performance testing
- ✓ User Acceptance Testing (UAT)
- ✓ Final commissioning
- ✓ System Architecture Documentation
- ✓ Configuration Documents
- ✓ Administrator Manuals
- ✓ User Manuals
- ✓ Standard Operating Procedures (SOPs)
- ✓ API Documentation
- ✓ License Documentation
- ✓ Test Reports
- ✓ Commissioning Reports
- ✓ As-built Documentation
- ✓ Training manuals, hands-on sessions and knowledge transfer documentation

12. Training & Knowledge Transfer

- ✓ Platform Administration

- ✓ User Administration
- ✓ Security Operations
- ✓ Threat Detection & Investigation
- ✓ Malware Analysis
- ✓ Incident Management
- ✓ Digital Forensic Operations
- ✓ Reporting & Dashboard Management
- ✓ Backup & Recovery
- ✓ Preventive Maintenance
- ✓ Basic Troubleshooting
- ✓ Administrator and user training
- ✓ Hands-on sessions, manuals, guides and knowledge transfer

13. Warranty, Support & Maintenance

- ✓ All applicable software licenses, subscriptions and activation keys shall be supplied.
- ✓ Five (5) years comprehensive OEM/software support or as specified in the BOQ.
- ✓ Software updates, security patches and version upgrades during the support period.
- ✓ Remote and onsite technical support, as applicable.
- ✓ Bug fixes, troubleshooting and incident resolution.
- ✓ Coordination with OEMs for issue resolution.
- ✓ Maintenance of the complete integrated software environment throughout the contract period.
- ✓ Module-specific support requirements in the technical specifications shall also apply.

14. 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

15. 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					

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

16. 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.

17. 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:

1. Supply / licensing of proprietary software or provision of open-source software components, as applicable.
2. Installation, configuration and customization of the proposed software solutions.
3. Integration and interoperability with the existing and proposed Cyber Operations infrastructure and other relevant departmental systems.
4. Development and implementation of required APIs, connectors, interfaces, workflows, dashboards and reports.
5. Testing, security validation, User Acceptance Testing (UAT), commissioning and performance validation.
6. Provision of all required implementation tools, middleware, connectors, documentation and technical components necessary for successful deployment.
7. Administrator training, user training, Train-the-Trainer (ToT) and knowledge transfer.
8. Preparation and submission of system architecture, configuration documents, user manuals, administrator manuals and SOPs.
9. Provision of applicable software updates, upgrades, security patches, bug fixes and technical support during the contract/support period.
10. 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.**

18. 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.

19. 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.

20. **Note to Bidders:-**

i) 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

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

iii) 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.

iv) 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.