**Tender No: 6300034088 Date: 03.09.2020**

# TENDER DOCUMENTS

# 

**REQUEST FOR QUOTATION FOR**

**CYBER-SECURITY OPERATIONS CENTRE (SOC) AT BEML SOUDHA**

**BID SUBMISSION DATE ON OR BEFORE 24.09.2020 BY 2 PM**

Pre issue co-ordination

DGM (ERP)

**BEML LIMITED,**

**Corporate Office,**

**BEML Soudha, 23/1, 4th Main, SR Nagar,**

**Bangalore - 560027**

# Introduction

BEML Limited is a leading public sector undertaking under the Ministry of Defence for manufacturing a wide range of Mining, Earthmoving, Railways and Defence Truck & Equipment.

BEML has decided to build a Cyber-Security Operation Centre (CSOC) to monitor, assess and defend BEML‘s information systems in order to protect confidentiality, integrity and availability of the BEML’s data.

The purpose of this Request for Quotation (RFQ) is to invite Bids from Bidders for setting up of a **On premise Cyber-Security Operations Centre(CSOC)** at BEML Soudha premises, supply and commissioning of tools as per requirements on a **turnkey basis and maintaining for 3 years after the warranty period**. The proposed CSOC facility is to be equipped with set of tools such as Security Information and Event Management Tool (SIEM), given in detail under this RFQ and Security Intelligence services for better security monitoring and response capabilities. BEML intends to implement On premise **Cyber-Security Operation Centre (CSOC)** for information assets at Data Center and Disaster Recovery center. BEML expect Service provider to provide full-fledged Services including but not limited to design, supply, implementation, configuration, customization, integration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEM and any other activities related to or connected to the Information Technology / Cyber security solutions, devices & technologies.

BEML would interpret a Security Operation Centre (SOC) as a centralized unit identified in an organization that delivers IT Security Services and deals with security issues of its branch offices at organizational and technical level. It attempts to thwart unauthorized access and manage security related incidents using processes and procedures and that it has distinct modules for event generation, event collection, message database, analysis engines and reaction management, and uses. **BEML reserves the right to cancel/ postpone the whole process based on its business priorities.**

1. **EXISTING INFRASTRUCTURE**

| **Location** | **Device Type** | **Device Vendor** | **Device OS Version** | **Number of Devices** | **Locations** |
| --- | --- | --- | --- | --- | --- |
| Bangalore | Servers - Sampark - BEML Connect - AD with Failover - DHCP - Biometric - CRM (production and quality) - Symantec - SAP Backup HP IRS Server |  |  | 12 | 1 |
|  | AV | Symantec |  | 2300 |  |
|  | Endpoints 2000 in AD |  |  | 2300 | 7 |
|  | Routers | Cisco & Juniper |  | 28 | 7 |
|  | Core Switches | Cisco & Juniper |  | 32 | 7 |
|  | Access Switches  These are unmanaged switches. However in future BEML is planning to replace these unmanaged switches to managed switches. | CE500 |  | 500 | All Locations |
| Bangalore | Firewall 2 networks Management Server | Check Point |  | 5 | 1 |
| Bangalore | Forward Proxy | Barracuda |  | 1 |  |
| Bangalore | Mail Server | Mdaemon (Windows) |  | 1 |  |
|  | SAP with ERP | HP UX Server | ECC 6.7 | 2- Bangalore 1- Mysore |  |
| Accessible through internet | ERP SRM (e-Procure) |  |  |
| SCM |  |  |
| FLM |  |  |
| Bangalore | Database multiple virtualization VMWare, HyperV | SQL |  | 2 (5+4) VMs | 1 |
|  | Applications |  |  | 6 |  |
|  | VAPT (in process of procurement) with half yearly with 512 IPs at a time. |  |  | 3000 |  |
|  | Asset & Patch management (in process of procurement) |  |  | 2000 |  |
| Bangalore | R&D Servers | HP UX Server | RX2628, UX 11.2 | 6 |  |
|  | R&D Servers | RHEL | RHEL 3.0 | 4 |  |
| Bangalore, Mysuru, KGF | R&D Servers CADD Licenses Storage PLM Domain controllers | Windows | 2003, 2008, 2012, 2016 | 57 | 3 |
| Bangalore | Internet Firewall  R&D BC Firewall | Cisco FHP 1140 & 1120 |  | 2 |  |
| Mysuru, KGF | R&D Firewalls | Cisco ASA 5510 | 7.2 and 8.0 | 2 | 2 |
| Marketing ROs/DOs | Fortinet Firewalls |  |  | 27 | 27 |

Currently BEML has a MPLS VPN network connecting all divisions to BEML Soudha Bangalore for Business Applications & an Internet Network for Internet connectivity across all divisions separately.

1. BEML, Unity Buildings, Bangalore
2. BEML, Bangalore Complex, Bangalore
3. BEML, KGF Complex , KGF, Kolar
4. BEML, BGML-KGF, Kolar
5. BEML, Mysore
6. BEML, Palakkad, Kerala

The detailed Network architecture will be shared to the successful bidder

1. **SCOPE OF WORK & TECHNICAL SPECIFICATIONS**

BEML Ltd has proposed to establish Security Operation Centre at **BEML Soudha (DC), Bangalore BEML Engine Division (DR), Mysore** for uniform implementation of cyber security polices and to establish single console for monitoring & administration of business network & internet network.

It involves the design and implementation of the Security Operation Centre, design of the operation frameworks, reports, templates, dashboards, security monitoring platform architecture, etc. and deployment of the tools / technologies to ensure a comprehensive deployment of SOC in BEML as defined in this RFQ.

The scope of work includes understanding the requirement, customizing and providing the deployment architecture of proposed solution. Supply, install and commission the respective appliances at BEML data center & DR Site. Configure the appliance for High availability (as specified in the technical specification), integrate the list of devices/appliances/applications etc. with the SIEM setup, tune up the appliances with BEML security requirement; document the solution, train the candidates nominated by BEML. This is not an all-inclusive list. The Bidder is expected to provide the end to end solution and vendor is expected to absorb any other cost of material / services if any to meet the specifications mentioned in this RFP. This is not an all-inclusive list. The Bidder is expected to provide the end to end solution and vendor is expected to absorb any other cost of material / services if any not particularly listed below.

The bidder should also provide **services** like Log analysis & Monitoring, Vulnerability Management, Application Security, Penetration Testing, Incident Management etc. as elaborated in this tender document.

Bidder should be able to integrate all types of security devices like DDoS appliance, Load Balancers, WAF, and APTs etc in future whenever BEML intends to procure these security appliances.

**Bidder will document all the pre-requisites, dependencies and best practices for implementing the Security Operation Centre and same should be managed by the bidder for a period of 3 years after expiry of warranty support of 1 year.**

The proposed SOC should be able to conduct detailed analytics and extract intelligence from the daily operations and activities occurring on BEML network. The bidder shall collect the exact requirement of putting the rules in place. These requirements shall also bring out the “Intent” of the rule is. It shall also capture the Reponses such a Rule would elicit. Once the requirements are captured, the bidder shall identify the logs to be used for creating the specific rules, what log attribute is more suitable for rule trigger, what are the various attributes to collect / represent, what type of alerting to be configured etc. Broadly, the bidder can classify the rules into the following:

* Single event rule
* Many to One or Many to Many Rules
* Cause and Effect rules or “Followed by” rules.
* Transitive Rules or tracking rules
* Trending rules
* Any other category

Based on interaction with BEML team, bidder shall time to time review the relevance of existing rules, identify and clean up old/obsolete rules and write new rules to keep up with the prevailing Threat Scenario.

Bidder shall also provide support in training, acceptance, documentation, management of all services and equipment of solutions, monitoring of incidents & logs, design and customize reports, warranty support and post warranty maintenance support for the Solutions.

The Bidder shall also provide support & services during transition of the SIEM and related services to BEML and/or its appointed new vendor for the same. The SOC solution must enable the BEML to collect, record, correlate, analyze, derive logical conclusion from logs, events, packet replay, provide malware analysis on information received by it from heterogeneous systems including Networking & Security systems, OS, RDBMS, Middleware, Web servers, Enterprise Management System, Active Directory Services, Corporate Internet Gateway, Mail Server, Antivirus and host of systems including applications spread across the BEML on 24x7 basis. The SOC infrastructure must support all features, functionalities etc. on real time and with 99.00% uptime on quarterly basis at each layer of solution for enterprise-wide infrastructure of the BEML including those operational at Data Centers. The Bidder shall integrate the SOC Solution with BEML’s information systems and security infrastructure.

Vendor has to do end-to-end configuration of the solution and implementation and customization as per best practices and BEML’s requirements. The vendor will ensure seamless integration of its equipments for functioning of existing as well as future gateway security appliances with no/minimum possible downtime.

The Bidder shall setup an onsite SOC at the BEML’s premises and provide the required security services for period of 3 years onsite support after expiry of warranty support of 1 year. The bidder shall train the in house personnel to run, manage, monitor, analyze and report incidents as they occur.

## SOC Deliverables

1. All the SOC activities should be automated (Basic log collection, storage, Archival, aggregation & correlation, case management has to be automated. In case of any further automation required in the future which shall be taken up on request).
2. Supply of the SIEM appliance/devices/products/licenses with provision for version upgrades/patches
3. Installation, Implementation and Integration of the solution as per the security architecture design; this will include device rules / device policy definition and enforcement on the devices proposed in the technical specifications.
4. Bidder shall also undertake to carry out implementation / operation including move, add, and delete changes / customization of such software updates, releases, Version upgrades. Bidder should update and maintain all supplied equipment to correctly reflect actual state of the setup at any point in time during the contract period
5. Configure rules / policies for correlation as per best industry practices and benchmarks but customized to the requirements of BEML to help identify potential security risks. The criteria for required rules and policies will be mutually discussed with the successful bidder during design phase of implementation.
6. Continually ensure 100% log sources of BEML Systems should integrate with proposed SIEM.
7. Continually audit all logs of all devices on daily basis and perform analytics to report anomalies as per response time specified in SLAs.
8. Bidder must ensure that the logs are collated, analyzed and acted upon as per the configured rules on the SIEM and report the appropriate severity level customized as the need may be.
9. Bidder should continually improve and fine-tune the SIEM deployment for the assurance of comprehensive integration of the required security and networking devices of BEML Network. Validation of the improvement must be accompanied by artifacts;
10. Bidder has to act as technical-advisor to BEML for SIEM systems by way of evaluation, demonstration, etc. as and when required by BEML. Vendor has to submit findings/reports to BEML and give suggestions/recommendations.
11. Continually create / update the Filters and Dashboards to enrich the monitoring & detection posture of the network and publish them as per the required frequency (daily, weekly, monthly, quarterly);
12. Perform Incident management and response; alerting, tracking, respond and closure.
13. Threat & vulnerability monitoring and reporting.
14. Provide detailed analysis reports identifying the correlation and patterns of incidents.
15. Continuously identify anomalies in order to identify persistent threats.
16. Training for Maximum of 5 and Complete Documentation to be given to BEML identified team
17. **Providing automated Backup and recovery mechanism for the Entire SOC solution including storage sizing for archival logs.**
18. Free updates to be carried out during the support period of **for a period of 3 years after expiry of warranty support of 1 year** after installation and commissioning
19. **Provide 3 years onsite support after expiry of warranty support of 1 year** from bidder after commissioning and installation of the SOC solution

**Providing ongoing software support, hardware maintenance, technical support and services for the entire SOC including hardware setup for a period of One Year (i.e. Warranty period) + Support period of Three years**

* All Hardware/Software will be installed in BEML premises and data on that hardware will be sole property of BEML. Bidder will not have any physical or logical access to this hardware except for some maintenance and repair work under BEML’s supervision. Bidder to ensure the strict adherence of DPSU information security guidelines.
* All the items should be delivered with Indian standard power cables.
* OEM helpdesk has to be available to bidder & end user both, 24x7x365 for support and complaint logging.
* Relevant portions, in the documents scanned & uploaded in pursuance of Eligibility criterion shall be highlighted. If the offer is not accompanied by all the documents, the same would be rejected.
* Any travel, boarding and lodging incurred by the bidder for supply, installation, integration, developing, testing and commissioning of the software shall be borne by the vendor himself.
* BEML requires the bidders to be capable of providing end-to-end solutions for their requirement, which includes delivering, developing/implementing, supply and installation of hardware, in liaison with BEML IT team and statutory bodies if any.
* The bid having the least “overall cost for BEML including 3 years support cost” will be considered for order placement. However BEML reserves the right to negotiate with L1 Vendor.
* BEML reserves the right to verify/ confirm all original documentary Evidence scanned & uploaded by Bidders in support of the eligibility criteria. Upon verification, evaluation/ assessment, if any information furnished by the Bidder is found to be false/ incorrect, their total bid will be rejected and no correspondence on the same shall be entertained.
* The Successful Bidder shall make own arrangements for transportation to & fro from their place during Installation and commissioning and during their period of contract.
* The Bidder should visit the site with prior appointment and carry out necessary inspection and test/measurement as are necessary before/after attending the pre-bid meeting and before submitting the bids. All costs associated with such site visit and in preparation and submission of the Bid will have to be bear by the Bidder. BEML Limited will in no case be responsible for such costs, regardless of the conduct or outcome of the bidding process.
* Bidders should indicate country of origin of all quoted items and submit the same as part of technical bid and if BEML feels items from any country is not preferable for security reasons the bidder should be able to procure the same from any other country of origin.
* The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and BEML Limited, shall be in English only.
* Hardware & software items are to be supplied and installed at **BEML Head Quarters Bengaluru (Data Center) & BEML Engine Division Mysore (DR Site).**
* All the quoted items should be on hardened Linux platform or equivalent including monitoring & reporting system.
* Delivery of material at site and installation including loading and unloading shall be the responsibility of supplier.

* The Bidder should inform acceptance of Purchase Order within seven days of receiving the order.
* Bidder has to deliver required nos. of fiber patch cords as per number of SFP+ & FC ports available in each of the items.
* Bidder has to quote premium level support (highest level support provided by OEM) from all applicable OEMs.
* Bidder / OEM need to submit escalation matrix for complaint logging and rectification.
* OEM L3 resource has to verify & review respective items after completion of installation & commissioning by bidder team.
* If multiple bidders are participating against same OEM, technical BOM should remain same for all bidders.
* The vendor should arrange for a comprehensive deployment audit done by OEM after completion of initial deployment and at the end of the deployment. The audit would be base lined against SOW, deliverables, BEML Policies and industry best practices. This would be linked to the payment against installation.

* No extra claim shall be entertained on account of all/part of any job redone on account of bidder’s negligence which results into damages/losses during execution of the job. Also, any component(s) required to deliver the solution after release of Purchase Order shall have to be provided by the successful bidder. All such cost shall be borne by the bidder.
* In case there is a cost incurred to BEML due the wrong BoM/Specification/feature-set of security equipment/device/appliance at any location, the same will have to be replaced by vendor at no extra cost to BEML.

## On-Premise Operation Team Specification

The asset list and service deliverables are provided in this RFQ for the bidder to assess the volume of work and accordingly finalize personnel with appropriate skills. The minimum team structure can be reviewed and revised periodically. The table lists the roles, skill sets of personnel required for the above deliverables. The Bidder may respond with additional resources apart from the minimum required based on its assessment of the scope of work, deliverables and SLA.

| **Role** | **BEML Requirement** | **No of resources required- On premise** |
| --- | --- | --- |
| Monitoring & Tracking Incidents/Alerts 10X6, Reporting & Escalation, Regular SIEM Administration (L1) | Qualification: Graduate Preferable Certification like CCNA/CCSP/ CEH/ Security OEM Certification on quoted SIEM solution Minimum 3-year of experience in IT Security. | 2 |
| Senior Security Analyst Incident Validation,  Incident Analysis,  Solution Recommendation,  Resolve Escalations,  Maintain Knowledge base,  Escalation point for device issue resolution, Patch  implementation, Rule base  Management, General SOC  Administration, Scheduling / Performing Scans, Submission Scan reports, Resolve  user queries. (L2) | Qualification: BE /BTech Preferable Certification like CCNA/CISSP/CCSP/ CEH/ Security OEM Certification on quoted SIEM solution  Minimum 5 - 8 year of experience in IT Security. | 1 |
| Offsite 24x7 Monitoring Resources – L3 as and when required. | L3 should be senior level SOC expert.  Should be able to handle end to end solutions for any Cyber attack incidents. | **-** |  |

* May be extended to 24 x 7 in future if and when required. Additional resources required for such support would be provided by the Bidder on chargeable basis. Cost for such additional Resources, if requested, for L1 and L2 would be based on the cost as quoted in the commercial bid for such resources.
* Bidder is required to submit the qualification, experience detail along with relevant technical certificates at the time of deployment to BEML.
* BEML reserves the right to conduct interviews of the proposed team members for CSOC operations.
* If any resource is absent, standby resources should be available. BEML may reject such manpower if BEML is not satisfied with his/her performance and payment will be made to bidder as per actual manpower support provided subject to adherence to SLA conditions.
* In case of resource replacement, bidder shall ensure proper Knowledge Transfer (KT) / handover is provided to new resource.
* Bidder shall ensure the Police Background verification of deployed resources at his cost and must provide to BEML Limited a copy of the same before deployment.
* The on-site L1 and L2 support may also be required to work on Sundays / BEML holidays or beyond office hours on working days in exigency, for which an advance notice will be given.

## PRODUCTS

**Security Information and Event Management**

The SIEM product must enable BEML to collect, correlate, analyse, derive logical conclusion from logs, events, information received by it from heterogeneous systems including Networking and Security systems, OS, Web servers, Mail Server, Applications, databases, other infrastructure etc.

1. The proposed SIEM/EDR solution should have integration with network and hosts discovery tools and be able to map the BEML System IT infrastructure on a real time basis;
   1. The proposed SIEM / EDR solution should be able to search for suspect files, handles, key contextual data in the BEML Network;
   2. The proposed SIEM solution must be able to scale at least additional 50% without requiring additional infrastructure additions during warranty period.
   3. The proposed SIEM solution must be able to connect to and conduct live forensic analysis on an individual host and / or end point;
   4. It must be able to collect information from compromised end points for analysis;
   5. The platform / solution must be able to remediate at scale viz kill processes, capture files, alert users, install patches and apply updates on real time basis;
   6. The platform / solution, in real time, must be able to point out programs that are leaking BEML System data through encrypted web sessions;
   7. The SIEM OEM should have registered office in India along with in-house support team based out of India dedicated to SIEM technology.
2. The bidder should have back-to-back support with the SIEM OEM. Bidder should not be a mere reseller but a systems integrator. Bidder must have prime and direct (selling, support, upgrade and service) partnership with the solution technology provider.
3. The Bidder’s proposed SIEM Solution shall be rated in Gartner magic quadrant for Security Information and Event Management as  leaders or challengers quadrant in any of the last three years for which this rating is published (or) the offered product shall be a domestically manufactured/produced cyber security product complying with the Indian government regulations/notifications regarding domestically manufactured/ produced products including requirements of Ministry of Electronics and Information technology (MEITY) notification reference File No. 1(10)/2017-CLES dated 02/07/2018. Proof of compliance to the above referred notification & Gartner’s Magic Quadrant shall be submitted as a part of technical bid.
4. The selected Bidder shall supply, install, customize, integrate, migrate, test, and troubleshoot the SIEM to run SOC; subcontracting or consortiums are not allowed.
5. The mentioned hardware pre-requisites are for SIEM tool only. For additional tools like PIM, MFA, NAC, IPS, IDS requirements tender will be floated in future. The SIEM tool should be capable of integrating other tools like Privileged Identity Management, Multi-Factor Authentication (PIM, MFA, NAC, IPS/IDS) etc., However these solutions will be procured in subsequent phases.
6. The proposed platform should be considered with given specifications as bare minimum and additional licensing options to be proposed which could be considered for procurement on need basis in future. The bidder‘s response should include the calculations/ logic used to arrive at the sizing.
7. Implement the SIEM tool to collect logs from the identified devices, applications, databases, end points, network devices etc., .
8. Ensure that the SIEM/ security monitoring and analytics tool & other solutions used in the SOC are up to date in terms of product releases, version upgrades, patches and other service packs.
9. The SIEM product must enable BEML to collect, correlate, analyse, derive logical conclusion from logs, events, information received by it from heterogeneous systems including Networking and Security systems, OS, Web servers, Applications, databases, other infrastructure etc.
10. Bidder must ensure that once the logs are written to the disk/ database no one including SIEM or database / system administrator should be able to modify or delete the stored raw logs .
11. Implement correlation rules based on out-of-box functionality of the SIEM solution and based on the use-cases defined.
12. The proposed SIEM solution should have built-in use cases along with open source Threat Intelligence Platform (TIP) integration capability.
13. The SIEM Solution should provide real time threat intelligence from own or other commercial third-party trusted feed vendors.
14. The SIEM tool should be integrated to VA Tool to provide a comprehensive dashboard for VA reports.
15. Monitor the SIEM alerts and suggest/take appropriate action.
16. Perform on-going optimization, performance tuning, and maintenance, configure additional use cases, and suggest improvements as a continuous improvement process.
17. The SOC team should configure the policies in the SIEM for automating the backup from SIEM to the NAS storage for archival retention policies.
18. Assisting BEMLs team for Cyber Drill activity conducted by CERT-In or any other agencies and also assist BEML for Audit conducted by CSG-MoD once in 2 years.
19. **Use Cases:** To ensure the SOC is effective, a series of Use Cases must be defined. For instance, a repeat attack from a single source is a Use Case. It’s an actionable component of the SIEM in which the SOC was notified of, through the SIEM Dashboard. A Use Case may include the involvement of a Rule, Alarm, or even a Dashboard to meet the organization’s requirements. The bidder shall define, develop and customize use cases in line with BEML policy, regulations & the technical environment.
20. The proposed SIEM solution should have built-in case management capability out of the box and integration with third party ticketing tool like serviceNow, Symphony Summit, SMAX Etc.
21. The bidder shall supply all the requisite hardware to ensure smooth functioning of the SIEM and other proposed components.
22. The SIEM shall be able to maintain, Online data = log data should be retained for 3 months and accessible to SIEM for analyzing & reporting at any point of time. Storage = Log data of 9 months beyond 3 months of online data must be stored in built-in storage and accessible to SIEM for analysis and reporting at anytime. The storage for these logs has to be proposed as a part of the bid. Archival = Log data aged beyond 1 year must be archived in compressed format in a different storage for a period of 4 years and the Hardware/Software required should be included in the vendor cost.
23. In case of non-availability of any remote log collector device, the logs of respective site have to be sent to DC (Bangalore) site automatically, without any manual intervention.
24. All the bidders should include required any HW & SW for centralized monitoring & administration of SIEM infrastructure proposed to be deployed as per RFP.
25. All the components of proposed SIEM solution at BEML including SIEM appliance, log collection devices, storage system should have hot-swappable dual power supply.
26. During the contract period, the faulty parts including disks must be replaced with new ones carrying warranty up to the total systems warranty end-date. Disks / backup media or any other storage media found defective & replaced during warranty period will not be returned to the Bidder.
27. Heavy Duty Racks (at least42U) for installation of all the hardware shall be supplied, with necessary power distribution unit, cable manager, Fan, front & rear perforated doors and rack kits.
28. All the related software / firmware updates, upgrades, patches etc., should be addressed for all the supplied BOM and shall be applied offline as the system are not available on public domain.
29. All cables & accessories to implement connectivity between Server, SAN switches, LAN switches, Storage will be provided by the bidder and install.
30. All the dashboards for SIEM monitoring should be completely customizable and shall have the feature for restricted access depending on user / group based. Dashboard should be hosted in BEML’s premises. The tool should provide flexible dashboard interface customized to user preferences allowing the examination of a specific event or a holistic view of the systems within the enterprise.
31. The solution shall be capable of automatically moving the logs from device to archival storage based on the ageing of the logs. The logs should also be available online to the device for easy correlation and auditing should provide detailed auditing to easily detect files deleted, add changes as and when asked by BEML.
32. The complete SIEM Solution shall have Write Once Read Many (WORM), Encryption, Advance Indexing and Searching, Retention and Disposal capabilities in Online, Near Line and External Storage Types.
33. The bidder shall customize reporting and security dashboards for BEML as and when required by BEML Security Team and shall have provision to sort/search as per requirement such as IP based, host based, etc.
34. The solution shall provide Compression and De-duplication functionalities on archival system.
35. The solution should be scalable as per BEML roadmap for expansion to integrate tools like PIM, MFA, IDS/IPS, DLP, NAC etc.,.
36. The solution should provide data replication over IP to a different site for disaster recovery and data protection with support for Unidirectional, Bi-directional, one-to-many and many-to-one replication topologies, Retention and Disposal functionality, and no single point of failure in the solution
37. Both Online & offline logs should be stored in built-in storage. Only for archival logs NAS storage shall be considered as per the 4 Year retention policy i.e., minimum 55 TB to be considered.
38. Successful bidder should consider at least following sample while initially setting up the SOC:
    1. Repeat attack from a single source.
    2. Repeat attack on a single ID.
    3. SMTP traffic from an unauthorized host.
    4. Antivirus failed to clean.
    5. Excessive SMTP traffic outbound.
    6. Excessive web or email traffic outbound.
    7. Excessive traffic inbound (streaming, web, etc.).
    8. Excessive access to a malicious website from a single internal source.
    9. Excessive connections to multiple hosts from a single host.
    10. Excessive exploit traffic from a single source.
    11. Excessive exploit traffic to a single destination.
    12. Excessive port blocking attempts from antivirus or other monitoring systems.
    13. Excessive scan timeouts from antivirus.
    14. Accessing a malicious website from multiple internal sources.
    15. Service account access to the Internet.
    16. Service account access to an unauthorized device.
    17. Scanning or probing by an unauthorized host.
    18. Scanning or probing during an unauthorized time window.
    19. Anomaly in DoS baselines.
    20. Anomaly in recon baselines.
    21. Anomaly in malware baselines.
    22. Anomaly in suspicious activity baselines.
    23. Anomaly in user access and authentication baselines.
    24. Anomaly in exploit baselines.
    25. Anomaly in network baselines.
    26. Anomaly in application baselines.
    27. Multiple logins from different locations.
    28. Multiple changes from administrative accounts.
    29. Multiple infected hosts detected on a subnet.
    30. Unauthorized user access to confidential data
    31. Unauthorized subnet access to confidential data.
    32. Unauthorized user on the network.
    33. Unauthorized device on the network.
    34. Unauthorized server connection to the Internet.
    35. Suspicious traffic to known vulnerable host.
    36. Logging source stopped logging.
    37. Logs deleted from source.
    38. Device out of compliance (antivirus, patching, etc.).

**Design a Security Reporting Framework:**

Bidder will design a detailed Security Reporting Framework with templates and dashboards for reporting to various stakeholders in BEML Network. The actual reporting will follow this Security Reporting Framework during Operations based on the activities in operations and maintenance phase.

This reporting framework and templates should contain at least the following reports /

dashboards:

1. Top 20 threats in BEML.
2. Top 10 non-compliances in the reporting period in BEML Network.
3. Internet facing systems and their usage volumes giving the cyber-attack surface exposed (should give all hosted BEML applications, web services running within BEML Network).
4. All at-risk network services running within BEML Network.
5. Exposure ratings for the exposed cyber-attack surface for each category.
6. Top 100 infected systems.
7. Top 100 infected users / Mail User Ids.
8. Top 20 account lockouts.
9. SIEM health status.
10. Top risks across globe, etc.
11. Count and details of incidents.
12. Top 10 latest/emerging threats/vulnerabilities / attack and threat vectors.
13. The Bidder will provide Online Dashboard for threat sources to be viewed by BEML Team. The dashboards shall cater to different views for management, senior management and top management.

**Integrate with Threat Intelligence Grids and Build Cyber Security Threat**

**Intelligence:**

The Security Threat Intelligence grid integration will be hardware independent – while

integrating with multiple threat intelligence sources to provide comprehensive advanced threat protection.

1. Bidder will prepare the threat intelligence dashboard with view events based on various criteria like geographical location, Device type, attack type, most attacked device etc. and blocking dashboard.
2. Bidder will close the incidents as mentioned in the SLA document.
3. Bidder will integrate the open source and subscribed intelligence feed and publish the advisories on the emergence of new global threat and vulnerabilities.
4. Any changes (if required from the fine-tuning of Threat intelligence report) will be done by the bidder.
5. Bidder will create the dashboard for the threats detection and the status of the remediation.

**SOC Case Management and Incident Response**

To enhance the functionality of the SIEM and SOC deployment, BEML also wants to procure Case Management tool for SOC. The feature-set required for the tool is mentioned in the technical specifications.

**Privileged Identity Management and Multi-Factor Authentication**

BEML wants to procure Privilege Identity Management and Multi-Factor Authentication solution in future in order to govern the remote users logging into BEML’s infrastructure and setup role, time and context based step-up authorization.

The proposed SIEM tool Hardware should be capable of integrating other tools like Privileged Identity Management, Multi-Factor Authentication (PIM, MFA, NAC, IPS/IDS) etc., **However these solutions will be procured in subsequent phases.**

**Security:** The Bidder shall not disclose any information pertaining to BEML. The password/encryption keys/other secrets should be kept confidential. The Bidder should provide the list of personnel handling the password/encryption keys/other secrets if any. They should adhere to the security policies established by BEML.

## SERVICES

**Security Operations Centre**

1. Bidder shall conduct the monitoring of various types of operating systems, web servers, application servers, Mail Server, databases, servers, storage, Network & security devices and solutions etc. Bidder will also be responsible for any escalation or trouble- shooting requirements.
2. The Bidder shall monitor onsite SOC at BEML’s premises during working hours **(0700-1900 hrs) for 6 days a week (Mon-Sat).**But during exigency, the vendor shall work on Sundays & Public Holidays with prior information from BEML. The Onsite resources (People, Process and Technology) required to run and manage the SOC shall be deployed from the bidder’s own **resources** to manage, monitor, analyze, mitigate and report incidents as they occur. The current requirement is of the mentioned quantities of resources only. Any amendments to the same can be taken up in the future on need with pro-rata basis.
3. Bidder shall monitor security devices/security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in BEML’s environment.
4. Bidder shall do pro-active and continuous monitoring of security events throughout the network by co-relation and analysis of logs from servers, network devices, security devices and application systems (Layer7)
5. Bidder shall do Log and availability monitoring for entire BEML infrastructure and business applications.
6. Bidder shall provide consolidated security status reporting through centralized and automated application.
7. Bidder shall provide centralized security dashboard with integrated reporting of all systems and services.
8. Bidder must follow the best practices for all compliances related to data and its security.
9. Bidder shall propose solution that should be able to retrieve the archived logs for analysis, correlation, reporting and forensic purposes. Forensic services (if required) shall be taken up on need basis. At the minimum, the bidder should assist BEML with historic data and basic analysis in case of an incident at no extra cost.
10. Bidder must ensure that for each security incidents, solution shall provide online and real time remediation guidance. The proposed SIEM solution should have out of the box content for ATT&CK MITRE framework. Default rules should be mapped with ATT&CK MITRE techniques.
11. Bidder shall submit Root Cause Analysis (RCA) report on the Major Information Security Incidents or for any incident, BEML desires to record RCA.
12. Bidder must provide threat intelligence feed (free or commercial off-the-shelf (COTS)) for identifying new global threats around the globe like DDoS (Slowloris or LOIC etc.), Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like latlong, ASNumber, ISP, Country, etc.
13. Bidder shall proactively inform about potential security threats/vulnerabilities, new global security threats/ zero day attacks / social engineering attempts in circulation and suggest and implement suitable countermeasures to safeguard BEML‘s IT assets and data against such evolving threats / attacks along with the analysis. Successful Bidder is expected to provide monthly security bulletin detailing the current threats and recommended mitigation techniques.
14. Operation team should send alerts with details to designate personnel and systems upon detection of anomalies. Alerts types at least should be, emails, phone calls, escalate the incident. The proposed SIEM solution should have built in case management, workflow management along with escalation capabilities. Currently Email will be the primary mode of notification however severity 1 incidents should also followed by a telephonic conversation with designated authorities. The detailed strategy for reporting and alerting incidents and findings along with the supported communication channels shall be shared with BEML Team.
15. Bidder should be adopting a variety of correlation methodologies that may include: a) Rule based Correlation b) Statistical Based c) Historical Based d) Heuristic Based e) Human Based Correlation.
16. Bidder must be able to correlate logs based on threat intelligence feeds for botnet command and control (C&C) servers, malware domains, proxy networks, known bad IP’s and hosts, traffic to APT domains.
17. Bidder shall develop custom plug-ins / connectors / agents for business application monitoring wherever required.
18. Bidder must monitor interruption or gaps in both generation and reception of logs, including missing logs, log disabled, log setting changes, time gap between log events.
19. Bidder must provide customized live dashboards with capability to browse and drill down to the actual data or other data transformations.
20. Bidder must provide capability to authorize IT staff to perform investigative advanced searches with rules and correlations over real-time and historical data.
21. **Integrate with Active directory** data to extract metadata on the users and assets to enrich the correlation. Such data would be department, previous department, employee type, and membership to groups, access to assets or criticality of the user, VLAN etc.
22. Bidder has to make sure that all the event logs from SIEM Security Analytics Database/Storage should be backed up at regular intervals on Monthly/Quarterly/Half year or as per the BEML’s requirement and Restoration drills for all the backup logs should happen every Monthly/Quarterly/Half yearly or as per the BEML’s requirement.
23. Bidder must ensure the integrity and confidentiality of the logs in transfer or at storage.
24. It should include the trend analysis comparing the present reporting cycle data with the previous reporting cycle data (Weekly, Monthly, Quarterly and annually as what may be applicable).
25. The successful bidder shall submit quarterly reports of the events encountered to the engineer-in-charge. The successful bidder shall also submit quarterly reports of equipment performance indicating equipment and disk space utilization.
26. The Bidder must benchmark the BEML Networks and suggest controls required to minimize impact from such attacks.
27. The Bidder will develop the systematic process to provide Early Warning of Threats.
28. **Bidder should develop a Standard Operating Procedure (SOP)** for all the products /solutions /services provided including alert management, incident management, Cyber fraud management, forensics, report management, log storage and archiving, Business Continuity.
29. **Prepare Cyber Fraud Management and Forensics SOP:** The Bidder shall prepare and deliver SOPs for Fraud Management and Forensic Investigation).

The SOPs for Fraud Management and Forensics should cover the following:-

**a**. **Cyber** **Fraud Management**

The Bidder will analyze and understand the BEML Network (rules, policies and

Business scenarios) and associated fraud risks. The Fraud Management SOP should

include at least the following:-

1. Suggest new tools which BEML should evaluate to mitigate recent and emerging fraud scenarios.
2. For conducting RCA of Fraud Incidents.

**b. Forensics SOP.**

The Forensics SOP shall include the workflow and activities initiating from the time

of incident

1. Logging till its closure with a detailed forensic report.
2. Develop new policies and improve the policies configured on an on-going basis to reduce the occurrence of false positives. Reference of policy in this clause is with regard to the monitoring, analysis and reporting of incidents in the SIEM platform.
3. Provide single integrated and consolidated enterprise view of security and compliance

**Management and Monitoring**

1. Bidder shall provide **(0700-1900 hrs) for 6 days a week (Mon-Sat)** management & monitoring of security devices which includes proposed devices. But during exigency, the vendor shall work on Sundays & Public Holidays with prior information from BEML.
2. The successful Bidder has to provide throughout the contract period, the services of an onsite L1 & L2 support personnel at Datacenter BEML Soudha, Bangalore the qualifications and Experience as described in this RFQ. As per the changing business needs, BEML may ask the Personnel to report for duty in different Time Windows as per the need of BEML.
3. Before updating critical systems and application, the criticality of the patch and the compatibility should be checked and the same must Management and maintenance of security devices / solutions/ technologies to ensure compliance with internal policies, regulatory & legal requirements be informed with corrective measures.
4. Reporting/escalations and closure of alerts shall also be configured in SOC
5. Crisis Management when incident happens shall be in place in concurrence with BEML’s IT Policy.

**Incident Response and Problem Management**

1. The bidder will also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate, recover and learn from the incidents responded to.
2. Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact.
3. The incident management solution shall be able to register any security event and generate alerts. The solution shall provide complete life cycle management of alerts from incident generation till closure of the incident. The solution shall have capability to structure rule-based workflow and calendar/ event based alerting capability.
4. Establishing process for identifying, preventing, detecting, analyzing& reporting all Information Security incidents as per the best practices, this may revise time to time as per the requirements.
5. Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the requirement.
6. Describe the incident response process including the roles and responsibilities and scope of action.
7. Incidence Response to comply with international standards including, but not limited to, ISO/IEC 27035-1 Security incident management NIST.SP.800-61 Computer Security Incident Handling Guide, CSIRT, Computer Security Incident Response Team.
8. Bidder shall do root cause analysis for security incidents and recommend implementation of controls to prevent reoccurrence.
9. Bidder must provide on demand timely support by performing investigation and forensic analysis on the logs by doing the necessary analysis on the logs and log review and providing required data on a timely fashion.
10. Faster incident response by replacing purely ad-hoc activities with Advanced playbooks, analytical tools, incident management tools and reporting, which liberates security analysts to spend less time doing research and more time doing analysis. (Please refer to section B of Annexure D.)
11. The Security Threat Intelligence grid integration will be hardware independent – while integrating with multiple threat intelligence sources to provide comprehensive advanced threat protection.
12. Bidder will close the incidents as mentioned in the SLA document.

**Forensic Rapid Response ( Need basis)**

The bidder need to provide the following in case of a security breach incident raised by BEML:- (as and when the incident occurrs)

* 1. Forensics domain expertise for evidence collection, investigation.
  2. The expert should be available at the site of the incident within 12 hrs.
  3. The expert should be available till completion of investigation and collection of artifacts along with detailed remedial plan of action against the investigation and handing over to regulatory authorities for further action.
  4. The expert should make himself available for supporting the investigation to BEML Team as well as to the regulatory authorities

**Penetration Testing**

1. The Bidder shall carry out PT for all public IPs (not exceeding 25) of BEML on a half yearly basis.
2. The Bidder shall conduct annually(yearly) penetration testing for identified devices / networks to identify security issues/vulnerabilities that could be exploited by remote attackers. The penetration testing exercise must give BEML a picture of overall security of the infrastructure as seen from the Internet.
3. The penetration testing should include testing for information pilferage, denial of service, password cracking, brute force attack etc.
4. The SOC shall Generate Executive Reports in graphical format and Technical Reports in text format for all penetration tests conducted.
5. Assessment document should necessarily contain proof/evidence of the vulnerabilities identified.
6. The Bidder shall provide a comprehensive report for Vulnerability Assessment and Penetration Testing activity. Vulnerability reporting must be concise and understandable. The Bidder shall provide / offer technical consulting services to mitigate the reported vulnerabilities. Once BEML initiates the corrective measures to mitigate the risk, a re-check shall be done by the vendor to ascertain / ensure the security of the organization. Bidder has to conduct regular VAPT for 25 external facing IP assets.
7. Bidder shall also conduct Social Engineering Assessment or also called Phishing simulation assessment every 6 months to identify vulnerable employees and get them trained on cyber awareness & hygiene.

**Firewall Assessment**

The successful Bidder is expected to conduct offline assessment of the firewall configuration every 6 months using industry standard tools. This should include post remediation assessment also. The Bidder shall carry out a half-yearly assessment of all the firewalls mentioned under **Existing Infrastructure** section. Detailed scope of this assessment is mentioned below:

1. Provide complete risk analysis by analyzing all possible traffic and Risk Identification from non- secured to secured zone.
2. Suggest consolidation of Rule Sets for optimizing the rules for better manageability, audit and performance
3. Scope of activities should ideally cover the below:
   * Identify unused rules
   * Identify shadowed rules
   * Identify disabled rules
   * Rule -level compliance checks
   * identify Redundant rules
   * Identify Time-inactive rules
   * Rules without logging
   * Rule usage information
   * Identify Risky access rules
   * Model firewall access paths
   * Root cause query in multiple-firewall multiple-vendor environment.

**Threat Hunting Service & Early warning of threats:**

The bidder shall build capability to identify and detect emerging, new & unknown threat vectors. This is in addition to identifying and detecting already known Threat Vectors (egg Phishing, Social Engineering, Anti-Phishing Services, Anti Rogue Services etc.). The intelligence that the Bidder builds in the SOC should be able to track an emerging threat pattern and prevent it before it manifests into an attack.

Bidder shall proactively monitor BEML websites for evolving threats. These evolving threats could be using known threat vectors or new threat vectors those are yet unknown and undocumented.

The Bidder should be continuously analyzing and discovering the following and any

combination of these and should provision reports to BEML:

* + Zero day threats
  + Known threats
  + Social engineering attempts

Any combination of the above Pro-active inputs in form of re-configurations, specific protective actions to be implemented on BEML System infrastructure in order to protect the network from any or all of the threat vectors described above or new zero day vectors.

The Bidder shall be responsible for the following activities:

1. Alert admin immediately if any such attacks are planned.
2. SIEM Solution should consume feeds from monitoring dark net forums / IRCs / chat rooms for BEML related activities, conversations, discussions, threats, etc. and provide reports of such activities, with artifacts;
3. Bidder must analyze application logs to identify transactions that are designed to be threats.
4. Bidder must assist BEML Network Administrator in coordination with law enforcement agencies to provide evidences that can be produced in courts of law etc., if required.
5. The Bidder must providing alerts on detection of threat sites, daily status report on the threat sources detected and the action taken.
6. The Bidder will provide Online Dashboard for threat sources to be viewed by BEML Team. The dashboards shall cater to different views for management, senior management and top management.
7. The Bidder will collect data, all assets, applications and database logs, reports, threat intelligence grids, logs from network devices, etc. as well as gather intelligence from third parties and perform analysis on them to implement the early warning system.
8. The proposed Early warning system should provide alerts but not limited to for following attack vectors:
   1. Detect zero day attacks.
   2. DDoS attacks.
   3. Advanced persistent threat.
   4. Any unauthorized data extraction, data transfer inbound/outbound, etc.
   5. BOT detection.
   6. Detect suspicious internal user, machine and network activities.
   7. Server access anomaly.
   8. Detect Malware lateral movement.
   9. External stealth attacks on web facing assets.
   10. External diversionary or noisy attacks on web facing assets.
   11. Alert Triage
   12. Risk Scores & Profile
   13. Any emerging attacks discovered as part of Threat Hunting (above).

**Anti-phishing Services:**

1. Create test scenarios and conduct social engineering of BEML System administrators and internal users (through phone calls, email, controlled attempts to breach IT, cyber and physical security) and ascertain the robustness of BEML Network preparedness.
2. Track new Domain Name Registrations to detect any spoofed or sites similar to BEML System domain being registered used and misused - this must include brand abuses too.
3. Upon detection, the Bidder shall work to trace, identify and shut down the source sites after due approval from BEML
4. The bidder must monitor web-server referrer logs, monitoring Spam traps, conduct Web site analysis.
5. The Bidder must analyze web server logs and application logs to track the phisher’s identity and bidder must be able to feed adequate number of wrong user-ids / passwords through automated tools to phishing site.
6. The Bidder should track the hosting of suspect and source sites through digital watermarks, initiate actions to take down of the suspect source sites / mailboxes / mobile apps / mobile stores on internet for the attack vectors.
7. 24x7x365 monitoring & mitigating/take-down of different phishing, pharming, Trojans, spyware, Brand-abuse, defacement of websites, etc. attacks on BEML’s IT infrastructure. BEML should get alerts in the event of above attacks on real time basis.
8. 24x7x365 monitoring of social media sites, FTP and distribution sites, grey markets, auction sites, job sites etc. for cases of brand abuse, BEML’s Trademark or Copyright property infringement.
9. The selected bidder should respond within 1 hour upon detection of any of the above attack and should work to shut down/take-down the detected site, anywhere in the world. The bidder should assist the bank in identifying customers affected by phishing attacks.
10. Gathering the Forensic information such as IP address, exact URL, source of attack, images, screen shots, email, account details, card details, compromised data etc. from the attacks and sharing the same with BEML.
11. Selected Bidder should have the reach on their own or through official business partnerships to take up closure/ mitigation measures on phishing sites anywhere in the world.
12. Track hosting of phishing sites through digital watermark, monitoring web-server referrer logs
13. Monitoring similar domain name registration - Track new domain name registrations to detect any spoofed or similar site being registered and shut down/take down the same.
14. Monitor spoofed email ids that may be used for sending emails to the customers of the BEML and take appropriate steps to protect the BEML’s interest.
15. Monitor anti-phishing forums.
16. Selected bidder should assist BEML for coordination with law enforcement agencies like National Critical Information Infrastructure Protection Centre (NCIIPC), CERT-IN, Cyber Investigation Research Agency-DRDO, Cyber Security Group, Ministry of Defence etc.,

**Documentation**

The bidder shall provide the following documents as part of the deliverables of the project.  
Original manuals of all proposed applications

1. System hardware and software details on CDs/DVDs as well as 01 hard copy.
2. 01 hard copy of the complete operating, configuration and maintenance Manuals and 02 soft copies of the same.
3. Besides these, the bidder shall provide the following documents:
   1. System interface drawings, if any.
   2. System interconnection drawings and block diagrams, if any.
   3. System built-up drawings, if any.
4. Standard Operating Procedures of installation and configuration documents
5. Architecture and design documents and troubleshooting manual
6. Executive summary report for the project to the management
7. Functional and operational requirements
8. Project design/plan
9. Product description
10. Guidance for best practices
11. Implementation guidelines
12. Business Continuity/ archival/ purging/back up policies/ procedures
13. Training material

**Continuous Improvement**

1. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.
2. Periodic health check should be carried out on-site, by the OEM every 6 months to ensure the quality of implementation and operations.
3. Bidder shall curtail the closure time for incidents and events, also ensure the periodic check-up reviews for the same.
4. Bidder needs to update all solutions and Cyber Security Operations Centre (CSOC) based on any new regulations and CERT-In guidelines and advisories.
5. Bidder has to integrate with proposed SOC at least 12 additional security devices/tools during the lifecycle of the project.

**Training:**

1. Successful bidder need to provide hands on training to BEML Team (5 Persons) for a period of 2 days on proposed system at BEML Bangalore premises.
2. Training should be on the following areas: Knowledge Transfer of the Deployed Solution Architecture and Design, hardware, software, integration, and customization, policy installation, troubleshooting process, creation of policies/rules, generation of reports, and analysis of the reports, troubleshooting and familiarization of features and functionalities, alert monitoring and other aspects of the solution.
3. In addition to above bidder should provide SIEM Training to BEML Team (5 persons) by faculty certified up to advance level with required practical experience and should provide courseware with adequate practical training. The training should be conducted by OEM for a period of 5 days.
4. The detailed training documents should be given to the training participants. The detailed theory & hands-on training should be imparted by the OEM personnel at BEML premises.
5. The training facilities shall be made available by BEML, the Bidder will have to ensure that training is imparted in a professional manner through certified and experienced personnel (other than on-site Personnel) and proper course-ware is given to every person attending the training.
6. Provide hands-on training on policy configuration, alert monitoring, Administration & Management of each component of the proposed solution.
7. Schedule of training will be finalized after having the confirmation from BEML.
8. Training should cover all the aspects of proposed system including administration, configuration, monitoring, troubleshooting etc.
9. Detailed training materials need to be submitted by successful bidder in form of CD /DVD /USB etc.
10. The bidder and OEM are required to provide ad-hoc trainings to the BEML staff as required by BEML, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. BEML has the right to exercise this training option at its discretion
11. All out of pocket expenses related to training shall be borne by the selected bidder.

**Service-Delivery and Project Management:**

The selected vendor will have to post a Service-Delivery Manager (SDM) immediately after the signing of the Contract. The detail of SDM should be conveyed in writing to BEML Limited within 2 weeks of receipt of purchase order. The Service-Delivery Manager will be required shall be available to BEML Limited, Bangalore. The SDM should have the following minimum profile:

1. Minimum 5 years of IT experience
2. He must aware and having knowledge of Service Delivery processes.
3. Minimum 2 years of Program Management experience.
4. 2 years experience of Network gateway security deployments.
5. Experience of handling/managing teams (Minimum 5 reportees).

The responsibilities of the Service-Delivery Manager as a part of support are as follows (indicative but not exhaustive):

1. Act as a Single Point of Contact (SPOC) for the entire project
2. Responsibility for the entire execution & management of the project after receipt of purchase order. (ii) Overall monitoring of project
3. Coordination for Delivery/Installation of New hardware in stipulated time frame
4. Call flow management, Quality Service Delivery
5. On-site Team management
6. Overall monitoring and management of network gateway security and related services
7. SLA management and reporting.
8. Submission of periodical Reviews and reports required by BEML.
9. Crisis management and Emergency response procedures.
10. Preparation and submission of detailed Project documentation to BEML (Purchase Order wise) and progress of initiatives taken by BEML.
11. He should be available to BEML whenever BEML expects right from the start of SOC Build till the project is entirely rolled out.

The Bidder shall submit to CIO, BEML the name and contact details, including address, telephone number, mobile number, FAX number/email address of the nominated Service-Delivery Manager.

It is mandatory for the concerned Service-Delivery Manager to have structured meeting with the CIO/DGM(ERP), at BEML Soudha BEML Limited once a week, during the implementation period from the date of receipt of the first Purchase Order by the vendor.

Weekly meetings should be held till the project is entirely rolled out.

In short, Onsite Service-Delivery Manager shall carry out and coordinate the various tasks involved in the project like Project scheduling, tracking, monitoring, identifying risks, liasoning with all stake holders (OEM, vendors’ back-end teams etc.) and reporting to BEML on the overall progress of the project, etc. No charges will be payable by BEML for the onsite

Service-Delivery Manager.

**Ownership & Licenses:**

Ownership of all hardware’s including networking devices and software developed/ customized/ configured/ procured for the BEML under this Project would lie with the BEML. All licenses of software/ hardware would be in the name of BEML i.e. BEML Limited with registered address at ‘BEML Soudha’ No. 23/1, 4th Main, S R Nagar, Bangalore – 560 027.

1. Licensing is the main part of any software based tools. Hence, proper licensing is the required for all software based tools.
2. The entire license should be valid for lifetime. However, the updation should be provided as per the warranty criteria. It is also to mention that all the licenses should exclusively be in the name of the user. In this regard a certificate from the OEM mentioning the end user and its validity period should be provided by the bidder.
3. All the licensing details also have been brought out at individual specification of the proposed tools.

# SOC Build

BEML will provide the space required for setting up of SOC. The Bidder shall visit the site before bidding with prior intimation to understand the setup. If the Bidder bids without site visit then any incidental charges will have to borne by Bidder himself.

Bidder shall take up the jobs related to site preparation of SOC Room- Flooring (Only tile flooring, not false flooring), Wall mounted TVs, and partition required, biometric access control, PCs for analysts, Air Conditioning with auto switchover, desks along with required power and network cabling. Further design requirements are as given below:

**Operator Desks- 6 Nos.**

1. Operator Desks shall be provided with suitable arrangement for placement of PCs. These shall have sliding trays for Keyboard & Mouse.
2. All cables shall be concealed with horizontal and vertical wire management accessories to give a neater look to SOC area.
3. Desk tops shall be made of MDF and clad with membrane foil using wrap around technology. The foil shall be pre-coated with poly-urethane layer for scratch and wear resistance.
4. The Desks shall be modular arranged in minimum 6 persons seating as per site requirements and space available.
5. Legs of the desks shall be profiled for better aesthetics.
6. Provide Biometric Access to the SOC Monitoring room.

**Operator Chairs- 6 Nos.**

Chairs shall be designed on Ergonomic lines suitable for seating of SOC Operators/ Engineers and continuous working on PCs. Operator Chairs should be from any reputed company make (Featherlite/Godrej/Wipro/Steelcase).

**Personal Computers- 4 Nos.**

The desktops provided for the analysts should have minimum Core i5 CPU, 16 GB RAM, 1 TB HDD, 24-inch full HD LED monitors, keyboard and mouse from a reputed OEMs (HP/Lenovo/Dell).

**Air Conditioners- 2 Nos.**

The ACs supplied should have adequate capacity to cover an area of 15ft x 20 ft. and should have auto switchover functionalities to distribute the wear and tear and shall be rated for 24x7 usage.

ACs required is 1.5 TR with Minimum Three star BEE rating should be from any reputed company make (Samsung/LG/Bluestar/Lloyd/Voltas/Godrej/Carrier/Hitachi/[Daikin](https://www.bing.com/search?q=Daikin&&filters=sid%3a%22f7070750-e42c-80c9-1c72-919fbd29966f%22+catguid%3a%22LCRQ_1B87E5923A9E46BEE0C5_e4272699-f7f9-4288-86a9-c07012acf67e%22+segment%3a%22generic.carousel%22+eltypedim1%3a%22Organization%22&FORM=LCHLRE)).

ACs shall include stabilisers for any voltage fluctuations in power.

**LED Displays- 2 Nos.**

The supplied LED displays (Television sets) should be of commercial grade with minimum screen diagonal of 55 inches and should be capable of running 24x7 along with necessary

mounting kits, Indian standard power cables.

**Biometric Access Control.**

The proposed SOC should have biometric access control. Only Authorized personnel should be given access to enter into SOC.

**Electrical.**

The Bidder shall supply and install all cables, adapters, power Cords and any other inter-connects for power and network required by the systems to meet the specification. The power adapter will be as per the Indian standard. The Bidder shall carry out all electrical and systems interfacing pertaining to equipments at SOC site as per the best international standards and practices.

The Bidder also shall do the proper lighting arrangements for ambience in the SOC room.

## GUARANTEE / WARRANTY :

Bidder has to have a back to back agreement with OEM to support the entire SOC solution for Six years (1+3+2).

1. The entire equipment/hardware (including OS) deployed for this project shall be under Comprehensive Onsite Warranty covering all parts including the display panel, updates, maintenance or support for its proper operation, performance and output as specified in the tender technical specifications for a period of 36 months from the Date of Acceptance or 39 months from the date of supply.
2. For Software (SIEM Tool & EDR) : The warranty will be for a period of one year.
3. For Services : 1 year warranty support & 3 years AMC support

## NDA & SLA

1. **After placement of order, successful bidder shall have to execute an Confidentiality Agreement / Non-Disclosure Agreement (NDA) on Non-Judicial stamp paper of value Rs. 200 as per the given format (Annexure – K) before or at the time of execution of the Contract. The costs and expenditure should be borne by the bidder**
2. During the contract period, the Personnel of vendor will have access to confidential information of BEML Limited such as IP addresses, router configuration, network security design, architecture, etc. The vendor or its Personnel shall not disclose at any point of time to any other person/third party the information so received and use the same degree of care to maintain the confidentiality of the information as if the information is their own. Also the vendor may use the information only for serving BEML’s interest and restrict disclosure of information solely to those employees of vendor having a need to know such information in order to accomplish the purpose stated above, advise each such employee, before he or she receives access to information, of the obligation of vendor under this agreement and require such employees to maintain these obligations. Violation of NDA will lead to legal action, forfeiture of PBG and blacklisting.
3. The selected bidder should execute agreement with the BEML which will remain valid until the end of this contract at the discretion of the BEML Limited. The agreement would include all the terms and conditions of the services to be extended as detailed herein and as may be prescribed or recommended by the BEML which will include a Non-disclosure Agreement clause.
4. The date of Purchase Order shall be treated as date of engagement and the time-line for completion of the assignment shall be worked out with reference to this date.
5. The Successful Bidder is required to execute a Service Level Agreement with BEML covering all terms and conditions of this tender. Bidders need to strictly adhere to the Service Level Agreements (SLA). Services delivered by the bidder should comply with the SLA mentioned in the RFQ and the scope of services mentioned herein above. SLA will be reviewed on a quarterly basis. The Bidder shall share SLA format as per conditions mentioned in RFQ with approval of BEML.

**Service Level Agreement:**

**Incident Management:**

There would be 10\*6 monitoring of all in scope devices and all critical, high and medium

priority events shall be logged as incident tickets as per below SLA:-

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident**  **Type** | **Rapid**  **Response** | **Update Time** | **Report with Root**  **Cause Analysis &**  **Corrective &**  **preventive plan** | **Penalty in case of failure** |
| Critical | 15 Mins | Within 30 mins | Within 48 hours | 10% of the quarterly Operations Cost |
| High | 30 Mins | Within 2 hours | Within 5 Days | 5% of the quarterly Operations Cost |
| Medium | 60 Mins | Within 12 hours | Within 10 Days | 5% of the quarterly Operations Cost |

1. In case of any security incident, bidder will share event logs along with action plan / mitigation steps to BEML team.
2. Bidder should detect both internal & external attacks. In addition to security attacks on IT infrastructure, Bidders should also monitor for security events on business applications, databases and also identify network behaviour anomalies.
3. Bidder should monitor, detect and manage incidents for the following minimum set of IT infrastructure security events:

- Buffer Overflow attacks

- Port & vulnerability Scans

- Password cracking

- Worm/virus outbreak

- File access failures

- Unauthorized server/service restarts

- Unauthorized changes to firewall rules

- Unauthorized access to systems

- SQL injection

- Cross site scripting

1. Bidder should monitor, detect and manage incidents for the following minimum set of

business application security events:

1. Attempted violation of defined role

- Attempted access violations

- Critical user additions, deletions

- Creation, deletion & modification of critical application roles/groups

- Changes to permissions or authorizations for critical application roles/groups

- Changes to account & password policies in the application

- Changes to critical application parameters

- Changes to audit parameters

- Sensitive data exposure

1. Bidder should monitor, detect and manage incidents for the following minimum set of network behavior anomaly events:

- Network Traffic Pattern Analysis and Bandwidth Analysis

- Host behaviors and traffic analysis to identify threats

- Analysis of traffic patterns & identifies nonessential ports and services for normal business operations

- Anomaly event as belonging to a class of security events (DDoS Scans, etc.)

**Service Level Agreement during warranty and AMC:**

The percentage uptime is calculated on monthly basis as follows:

(Total Hours in a month – (minus) Downtime hours within the quarter)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ X 100

Total hours in a quarter

In case of any hardware problems, the bidder should ensure the FREE replacement of the devices to meet the SLAs.

The SOC operation charges includes: equipment AMC, resource cost for AMC monitoring &

maintenance.

Down time: Down time is defined as time between the time of report by the BEML and time of

restoration / rectification within the contracted hours. “Failure” is the condition that renders the solution is not available to the BEML.

If the bidder fails to maintain the guaranteed uptime, penalty based on Level of availability of

uptime will be deducted as under:

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl.**  **No.** | **Description** | **Required Uptime** | **Penalty**  Penalty as xx % percentage  (as mentioned below) of overall monthly SOC operation charges. If the up  time is below 70%, BEML will have full right to terminate the contract with the Bidder. |
| 1 | SIEM, Storage,EDR, Incident  Management tool, log collection system ( deployed both at Bangalore & Mysore BEML) | 97% and above | N A |
| 95% to 96.99% | 5% of Notional AMC  charges for each failure  *(Refer A below)* |
| 90 % to 94.99 % | 10 % |
| 80 % to 89.9 % | 20 % |
| 70% to 79.9% | 30 % |
| 60% to 69.99% | 50% of Notional AMC  charges for each failure |
| Less than 59.99% | 100 % |

1. For hardware/software items whether under AMC or under warranty/free support, notional AMC/License fee shall be calculated at 10% of the asset value or their actual AMC cost quoted after expiry of warranty period, whichever is higher, will be considered for the purpose of calculating penalty.
2. For repeat failure, same or higher penalty will be charged depending upon the delay in rectification of the problem.
3. Penalty will be calculated on Quarterly basis and deducted against the Quarterly payments.
4. All the penalties shall be capped to 5% of the Total Contract Value.

**Exclusions from downtime calculation include the following:**

Downtime because of LAN cabling faults.

Scheduled downtimes (which are ***approved by BEML***) on account of preventive maintenance, system testing, system upgrades etc.

All failures due to source power unavailability and power conditioning, UPS failure etc. beyond control of Bidder Managed Services.

Force Majeure conditions defined above or any condition not foreseen but mutually agreed by both the parties.

Link outages owing to ISPs.

Downtime due to any device/appliance not managed by the Bidder.

# time lines/Delivery Schedule

* Detailed project plan with PERT chart and justification considering relevant skill set should be submitted before project kick-off meeting.
* All activities should be completed within 22 weeks from the PO date.
* A Project Kick-off meeting should be held within 1st week of placing PO to finalize the

implementation schedule. Indicative implementation schedule as mentioned in this RFP.

* Installation & Commissioning include the successful completion of the following activities:
  + 1. Deployment & configuration of respective devices as per the specifications & requirements mentioned in RFP
    2. Demonstration of the same by bidder to BEML Team.

|  |  |  |  |
| --- | --- | --- | --- |
| **Timeline** | **Activity** | **Milestone** | **Bidder Deliverables** |
| T0 | Placement of Purchase Order |  |  |
| T1 (T0 + 8 weeks) | Delivery of hardware | 1st Sign-off | * Delivery of hardware to respective locations. |
| T2 (T1 + 4 weeks) | Setup and installation | 2nd Sign-off | * Setup and installation of required Hardware & Software. Configuration of the  Setup * Network Configuration |
| T3 (T2 + 6 weeks) | Integration and content development | 3rd Sign-off | * Deployment of Onsite Resources * Integration of All Devices except (R&D Infrastructure) * Develop Standard Reports (At least 8) * Submission of   + Implementation Document   + Warranty Support Document   + SLA |
| T4 (T3 + 4 weeks) | Integration of R&D Infrastructure | Final Sign off | * R&D Infrastructure Integration |

# LOCATION :

The main Security Operations Centre hosting technology and people for the BEML is located at **Datacenter, BEML Limited, BemlSoudha, No. 23/1, 4th Main, S. R. Nagar Bengaluru – 560 027** and **DR Site is located at BEML Limited, Engine Division, Belavadi Post, Mysore – 570 018.**

# Scope of Acceptance testing and commissioning

After installation and configuration of each and every subsystem, integrating various systems and providing various services, tests shall be conducted for system performance as a whole

1. The deliverables are considered as accepted once the hardware components are delivered and installed at our SOC with the acceptance letter issued by BEML IT Team. This shall be shown through the server console and screen shots of the same shall be provided as documentation.
2. Commissioning shall mean end-to-end commissioning of the product with testing of live applications. Test parameters, commitments etc., shall be submitted along with implementation plan, which shall be approved by BEML.
3. In the event, the test parameters, commitments are not submitted or not accepted explicitly in writing/minutes by BEML, the Test parameters, commitments etc. as decided by BEML will be final and binding.
4. Upon Self-testing and Commissioning, the system shall be offered for inspection by BEML.
5. The successful Vendor, along with BEML shall prepare an inspection and acceptance schedule with details of each activity.
6. **Transportation:**

The Bidder shall transport/deliver goods to the BEML's premises as per delivery schedule. BEML shall not pay separately for the transit insurance and it is the responsibility of the Bidder to ensure that goods arrive at the destination in good condition. Bidder is also required to clear the goods for exporter etc. The following clause will form part of the contract placed on successful bidder:

* 1. On receipt of consignment, the Packing cases should be opened, for checking visually and Transit Damages, if any, by the BEML.
  2. Transit Damages, if any, should be reported by the BEML to the Bidder within 30 days from the date of receipt of consignment failing which no claims will be entertained by the Bidder.
  3. In event of transit damages occurring; the BEML's report should include the following information:-
     1. Date of receipt of stores
     2. Date of inspection
     3. Consignment / Carrier delivery note number
  4. The Bidder shall undertake to repair / replace the damaged / deficient items as early as possible.
  5. The contracted goods shall be insured by the Bidder in favour of the BEML as per BEML purchase procedure.
  6. Unless applicable, no part shipment of goods would be permitted. Transshipment of goods would not be permitted. In case it becomes inevitable to do so, the Bidder shall not arrange part-shipments and/or transshipment without seeking prior written consent of the BEML. Bidder will be required to communicate the following information invariably in advance before the shipment point of bidder for any consignment under this contract:-

1. Name of the Carrier / Ship
2. Name of Loading station and Country
3. ETA at BEML's premises / port of Discharge
4. Number of Packages and weight
5. Nomenclature and details of major equipment
6. Special instructions, if any stores of sensitive nature requiring special attention

**Packing, Marking and Dispatch:**

The Bidder shall ensure correct packing, marking and forward the goods to the destination indicated by the BEML. The following Packing and Marking clause will form part of the contract placed on successful Bidder –

1. The Bidder shall provide packing and preservation of the equipment and spares/goods contracted so as to ensure their safety against damage in the conditions of land, sea and air transportation, transshipment, storage and weather hazards during transportation, subject to proper cargo handling. The Bidder shall ensure that the stores are packed in containers, which are made sufficiently strong, and with seasoned wood. The packing cases should have hooks for lifting by crane/fork lift truck. Tags with proper marking shall be fastened to the special equipment, which cannot be packed.
2. The packing of the equipment and spares/goods shall conform to the requirements of specifications and standards in force in the territory of the Bidder's country.
3. Each spare, tool and accessory shall be packed in separate cartons. A label in English shall be pasted on the carton indicating the under mentioned details of the item contained in the carton.
4. Part Number:
5. Nomenclature:
6. Contract annex number:
7. Annex serial number:
8. Quantity contracted:
9. Carton No
10. One copy of the packing list in English shall be inserted in each cargo package, and the full set of the packing lists shall be placed in Case No.1 painted in a yellow color.
11. A complete / full set of packing lists should be provided to the BEML before 10 working days of arrival of consignments at the port / airport of destination. If necessary, each package shall be marked with warning inscriptions: <Top>, Do not turn over, category of cargo etc.
12. **Turnkey Approach** : The contract is one in which the vendor delivers, installs, implements, maintains and passes an acceptance test, training and documentation.
13. **Subcontracting:**

1. As per scope of the RFP, subcontracting is prohibited. However, if the Bidder subsequently wishes to sub-contract the scope of work, it will have to obtain specific written permission from the BEML before contracting any work to subcontractors. BEML at its own discretion may permit or deny the same.
2. In case subcontracting is permitted by BEML, the bidder will be responsible for all the services provided to BEML regardless of which entity is conducting the operations. The bidder is also responsible for ensuring that the sub-contractor comply with all security requirements of the contract and BEML can obtain independent audit report for the same. In such a case, the Bidder shall provide subcontracting details to BEML and if require, BEML may evaluate the same.
3. **RFP INTERPRETATION**

**Interpretation of the wording of this document shall be the responsibility of BEML and that interpretation shall be final.**

BEML shall not be liable for any costs incurred by any bidder in preparation, submission of documents in response to RFP and conducting /presenting demonstration of capabilities of such solution in response to this RFP.

1. **SPECIFICATION:**

The Bidder confirms that the goods to be supplied under this Contract shall conform to the technical specifications mentioned in this contract. In case no standard is mentioned, such standard shall be the latest issued by an authoritative institutions or a standards body of international repute. All goods to be supplied shall be new, state-of-the-art and of outstanding workmanship.

1. **PROCEDURE FOR SUBMISSION OF BIDS**

You are required to submit bid in three parts viz. (1) Pre-Qualification bid, (2) Technical Bid and (3) Commercial Bid. BEML may at its sole discretion amend the bidding documents at any time prior to the deadline for submission of bids. However in case of such amendment, the bid submission date may be extended at the discretion of BEML. Amendments made prior to submission of bid will be provided in the form of corrigendum to the bidding documents and will be posted on the BEML website (<http://www.bemlindia.com/tender_hq.php>)

**Note:** To participate in this e- tender you should have a valid Class III Organization Digital Signature with Signing and Encryption issued by authorized Certifying Authority.

Bidders willing to participate in the tender may contact through e-mail: [admin.srm@beml.co.in](mailto:admin.srm@beml.co.in) to obtain the user name & password for submitting the bids.

In case of any queries relating to bid submission, you may send the same by e-mail to [admin.srm@beml.co.in](mailto:admin.srm@beml.co.in) or you may contact BEML SRM Team on phone no. 080-22963269/141.

**Part A –** Submission of Pre-qualification Bid i.e. Submission of EMD amount (In manual Mode / Online payment Mode)

**Part B –** Submission of Technical Bid (Through e-mode on BEML SRM system)

**Part C –** Submission of Price Bid (Through e-mode on BEML SRM system)

**PART A – PRE-QUALIFICATION BID :- The EMD amount can be submitted in either way as detailed below at i, OR ii a) OR ii b) or ii c), :**

As a part of Pre-Qualification process, bidder needs to furnish the following by post/ courier or by hand before closing date and time of the tender:

1. **Online Payment of EMD amount can be made as mentioned below**:
2. Open the following link:<https://www.onlinesbi.com/sbicollect/icollecthome.htm?corpID=9359>
3. Read the terms & conditions, tick the acceptance box and click on Proceed.
4. In ‘Select State’ dropdown, select All India and click on the Go button.
5. In ‘Select Payment Category’, select EMD/ Tender Fee.
6. Enter details of payment, details of Bank Account for refund and click on Submit to make the online payment of the required EMD amount of Rs. 8,00,000/-.

**Please ensure that online payment of EMD amount is made well ahead of the Tender Closing Date & Time mentioned in the Tender.**

1. **Payment of EMD amount through DD / Banker’s Cheque**
2. EMD in the form of Account Payee Demand Draft (DD) / Banker’s Cheque for Rs. 8,00,000/- (Rupees Eight Lakhs only) drawn in favor of BEML Ltd, Bangalore payable at Bangalore.
3. Bidders exempted from Earnest Money Deposit (EMD) shall submit exemption certificate from competent authority.
4. An irrevocable Bank Guarantee from a Scheduled Commercial Bank authorized by RBI to issue a Bank Guarantee in favour of the Purchaser as per format in **Annexure-A** having a validity period of bid validity + 45 days from the date of opening of Tender.

Please attach the details duly filled-up for refund of EMD amount in the following format along with the DD / Banker’s Cheque for EMD:

|  |  |  |
| --- | --- | --- |
| **Sno** | **Particulars** | **To be filled & submitted along with DD/Banker’s Cheque** |
| 1 | BANK NAME |  |
| 2 | BRANCH NAME |  |
| 3 | CITY |  |
| 4 | IFSC CODE |  |
| 5 | ACCOUNT NO |  |
| 6 | BENEFICIARY NAME |  |

1. Duly signed Integrity Pact (I.P.) **in original** along with its enclosure. All pages of Integrity Pact including its enclosure to be signed with company seal by the Bidder. Two witnesses are also required to sign indicating their name and address at the designated place in the Integrity Pact.

Bidders who are interested to participate in this tender are required to enter into an **“Integrity Pact”.** The Integrity Pact envisages an agreement between the prospective vendor/ Bidder and the buyer committing the persons/officials of both the parties not to exercise any corrupt influence on any aspect of the contract.

Only those vendors/ Bidders who have entered into an Integrity Pact with BEML Limited would be eligible to participate in the Tender with BEML. The specimen of the Integrity Pact which is part of tender documents is enclosed at **Annexure-B** and same has to be duly filled and signed with seal by the Bidders on all pages along with witnesses’ signatures indicating their names and addresses.

The Central Vigilance Commission (CVC) has appointed Shri Ajai Kumar& Shri Virendra Kumar Saksena as Independent External Monitor (IEMs) to oversee the implementation of the Integrity Pact. Address of IEM is as below:-

Shri Ajai Kumar

2601, Tower–C,

Ashok Tower, Parel,

Mumbai - 400 012.

Mobile no.09619272893

Email :[Ajai.kumar3@gmail.com](mailto:Ajai.kumar3@gmail.com)

Shri Virendra Kumar Saksena, IRS (Retd.)

Flat No. 001, Tower CMC-3,

Cape Town Supertech, Sector – 74,

Noida – 201301

Mobile no. 08800713311

Email : [vksaksena\_irs@hotmail.com](mailto:vksaksena_irs@hotmail.com)

The Integrity Pact (Annexure – A along with Enclosure to Annexure - A) to be submitted along with EMD as **“PRE-QUALIFICATION BID” on or before closing date of the tender i.e. 24.09.2020 by 2PM to the following address**

The above said Demand Draft DD / Banker’s Cheques / EMD Exemption Certificate / Bid Guarantee form and Integrity Pact (Annexure – A along with Enclosure to Annexure - A)shall be submitted in **Sealed envelope** duly superscribing the **Bid Invitation No. 6300034088 dated 03.09.2020**, **Closing date 24.09.2020 Time 14:00 Hrs** at the top of the envelope. The words **“PRE-QUALIFICATION BID”** shall also to be written in bold letters at the top of the envelope. The name and address of the bidder shall be printed or written legibly on the left hand bottom corner of the envelope.

**Pre-Qualification Bid has to reach the address as mentioned below on or before the closing date & time of the tender.**

**The General Manager,**

**Corporate Materials.**

**BEML LTD,**

**BEML SOUDHA,**

**23/1, 4th Main, S.R. Nagar,**

**Bangalore – 560 027**

**KARNATAKA, India**

Alternatively it can also be dropped in the Tender Box which is kept in Room No.2, Ground Floor, BEML Soudha, SR Nagar, Bangalore.

The Bidders who have not submitted **“EMD(form of DD/ online / EMD Exemption Certificate / Bid Guarantee form) and Duly signed Integrity Pact” by the closing date & time of the tender will be rejected straightway.” Also bid submitted with EMD in the form other than Demand Draft** / **Banker’s Cheques will be rejected straightway.**

1. The above sealed envelope has to reach the address as mentioned below on or before the closing date & time of the tender.

General Manager (Corporate Materials)

**BEML LIMITED**., Room No.2

BEML SOUDHA, 23/1, 4th Main,

S.R. Nagar,

Bangalore – 560 027

KARNATAKA, India

**Alternatively it can also be dropped in the Tender Box which is kept in Room No.1, Ground Floor, BEML Soudha, SR Nagar, Bangalore**.

**Note**: Bidder shall ensure that their EMD (DD)/EMD Exemption Certificate/Bid Guarantee for and Integrity Pact is dispatched well in advance so that it reaches this office before the time and date stipulated. Requests will NOT be entertained for late receipts.

**General Instructions with regard to EMD:**

1. Quotation submitted online without submission of EMD/EMD Exemption Certificate in-time will not be considered.
2. EMD submitted in any other form will not be accepted and the offer is liable to be rejected.
3. EMD lesser than Rs.8,00,000/- will not be accepted and the quotation is liable to be rejected.
4. EMD of technical disqualified bidder’s will be returned.
5. EMD of unsuccessful bidders will be returned after finalization of the contract and the EMD of successful bidder will be released after submission of Performance Bank Guarantee / Security Deposit.
6. EMD does not carry any interest on return.
7. EMD will be forfeited if any firm withdraws the tender submitted or refuses to execute the order for reasons whatsoever.
8. EMD in the form of online payment is to be made before the bid closing date and time. EMD in the form of DD / Banker’s Cheque or NSIC certificate, MSME Certificate (firms claiming EMD exemption),BID Guarantee Formand Integrity Pact to be submitted through Courier / Post in a sealed cover, superscribing the bid number and closing date, address etc. before the bid Closing Date & Time. Failure to do so will result in rejection of the bid.
9. Tender will be opened on closing date at 15:00 hrs in presence of bidders who wish to be present.
10. No responsibility will be taken for postal or non-delivery/non receipt of EMD/firms claiming EMD exemption.

**Forfeiture of Earnest Money Deposit (EMD)**

1. EMD will be forfeited if any firm withdraws the tender submitted or refuses to execute the order for reasons whatsoever.
2. If there is any breach of terms and conditions of the contract on part of the successful bidder after award of contract.

**PART B – Submission of Technical Bid (Through e-mode on BEML SRM system)**

Please upload the following documents in the Collaboration Folder in the system as part of Technical Bid .

Bidders will be technically qualified based on providing documentary proof for each of the below eligibility criteria clause along with the Technical Bid

**Ref. No. 1 to 6 are mandatory terms. If bidder is not complying for these clauses or not uploaded required documents, their bid will be rejected straight away and no further correspondence will be entertained from the bidder.**

**However details for remaining non mandatory clauses (Sl no.7 to 16) also to be uploaded. In case any document / clarification are required for these non-mandatory clauses by Technical Evaluation Committee, the same shall be asked from the bidders before opening the Commercial bid.**

**Table : Technical Bid**

| **Sl No** | **Criteria Details** | **Documents required to be uploaded in Collaboration folder of SRM system** |
| --- | --- | --- |
| **MANDATORY** | | |
|  | Brief Details about the Firm | Please upload filled-in format as per **Annexure - C.** |
|  | The Bidder should be authorized / certified partner of the OEM. The Bidder must be in position to provide support / maintenance / up gradation during the entire period of contract. | Manufacturer Authorization Form (MAF) from OEM to be uploaded |
|  | The Bidder should have experience in supply, implementation, support and managed services of captive SOC with SIEM for any PSU / BFSI /Government / Enterprise customers in India. SOC solution with SIEM **(mandatory)** and should have at least 2 out of the following components apart from SIEM like Firewall, AAA (Authentication), WAF, DAM, PIM, NBA, Anti-APT solutions/Anti-Phishing, DLP, MDM, Anti-DDoS, NAC, and Vulnerability Management in the last 5 years  a. Three similar completed works costing not less than **Rs. 1.60 Crores**  Or  b. Two similar completed works costing not less than **Rs. 2 Crores**  Or  c. One similar completed works costing not less than **Rs. 3.20 Crores** | (PO / Work Order Copy related to establishment of SOC along with Completion certificate from the customer) or (PO Copy/Work Order related to establishment of SOC along with proof for completion of the work from the customer like invoice and payment details to the bank clearly mentioning the invoice details with reference to the PO). |
|  | The Bidder should be ISO 9000/9001, or ISO/IEC 27001certified, with certifications valid at the time of bid submission. | Documentary proof i.e. photocopies of certificates to be uploaded |
|  | Technical Specification of SIEM & SOC compliance sheet | Please upload the filled, signed & sealed technical Specification sheet as per **Annexure – D** |
|  | An Undertaking has to be submitted by the bidders stating that they have read, understood and agreeing to all tender terms and conditions. | Undertaking document as per **Annexure – E** to be uploaded in the collaboration folder. |
| **NON MANDATORY** | | |
|  | Average annual financial turnover during the last three years, ending 31st March of the previous financial year (i.e. 2017-18,2018-19 & 2019-20) should be minimum **Rs. 02 Crores** | 2017-18 Rs.  2018-19 Rs.  2019-20 Rs.  Copies of audited balance sheet (indicating turnover) for last three years shall be uploaded in the collaboration folder.  **Note:** If the audited balance sheet for the FY 2019-20 is under audit, then provisional balance sheet to be provided otherwise the average annual turnover during the previous three years shall be considered for evaluation i.e. 2016-17, 2017-18, 2018-19. |
|  | The bidder should be a registered corporate in India registered under the Companies Act, 1956 or a company/statutory body owned by Central / State Government. | Certificate of Incorporation |
|  | Desirable Technical Specifications of SIEM | Please upload the filled, signed & sealed technical Specification sheet as per **Annexure – F** |
|  | Technical specification for Display Unit | Please upload the filled, signed & sealed technical Specification sheet as per **Annexure – G** |
|  | Bidder / OEM should have their own SOC located in India | Self-Certificate with address |
|  | The bidder should have minimum 25 skilled staff with professional certifications like PMP/ CISSP / CEH / CCSP / CCNA/JNCIA/ISMS Auditor/CRE or Security OEM trained for SIEM, out of which at least 2 resources should be deputed for BEMLs SOC project | List of skilled staff with their Technical Qualifications and Self-Certification for the same to be uploaded |
|  | The bidder/OEM must possess all valid certificates as mentioned below and should upload copies of the same:   * + - * 1. PAN Number         2. GST Registration details/ Certificate | Please upload scanned copies of   1. PAN Number 2. GST Registration details/ Certificate |
|  | The vendor should not have been blacklisted by any government/ PSU/Reputed Listed company for corrupt or fraudulent practices or non-delivery, non-performance. | Undertaking document as per **Annexure – H** to be uploaded in the collaboration folder. |
|  | Special Conditions arising out of implementation of GST Tax Indemnity clause | **Annexure – I** to be signed and uploaded in the collaboration folder. |
|  | Bidder has to upload compliance sheet as part of the technical bid. | Please upload **Annexure – J** |

**Note:**

(1) The Bidders must ensure that the documentary proofs to substantiate clauses above are given, without which their bid will not be considered.

(2) Relevant documents are to be meticulously uploaded by the bidder and the bid will not be considered if any of the documents is not uploaded.

(3) Please **ensure that no price details are mentioned in the technical bid** (attachments to the Collaboration Folder). Offers with price details in Pre-Qualification Bid (under Part A) or Technical Bid (under part B) will not be considered.

(4) Technical bid will be opened first subject to receipt of original DD for EMD **OR** EMD Exemption certificate**/**document and Integrity Pact as **Pre-qualification bid**. If bidder is not submitted any of these (DD or EMD exemption certificate**/**document and Integrity Pact) in a sealed cover as **Pre-qualification bid**, their technical bid will not be considered for further evaluation

**PART C – Submission of Price Bid (Through e-mode on BEML SRM system)**

**Price Bid:** Should contain price details and other relevant Commercial issues.

Price bid to be submitted through E-mode as per the following format by clicking on item data tab in SRM.

| **Sno** | **Description** | **Qty** | **Basic Price in Rs.** | **GST%** |
| --- | --- | --- | --- | --- |
| 1 | Log Collection Server - 1 each for DC & DR | 2 Nos | No price bid to be filled here. Price bid to be uploaded on SRM Platform Only | |
| 2 | Log Management Server - 1 each for DC & DR | 2 Nos |
| 3 | Log Correlation Server | 1 No |
| 4 | EDR Management server | 1 No |
| 5 | Packet Capture solution with 15 days storage | 1 No |
| 6 | Storage | 1 No |
| 7 | Endpoint detection and response (EDR) On-Premise | 600 Nos |
| 8 | SOC Build ( Total Package) | 1 No |
| 9 | Implementation Cost | 1 AU |
| 10 | SIEM Licenses (As per Technical Specifications) for 3000 EPS | 1 No |
| 11 | Resources Cost ( for 3 Personnel) per year | 1 No |
| 12 | AMC for 3 years - after warranty period of one year | 1 AU |
|  | **Total Cost** |  |
| **13** | **SIEM (Additional 1000 EPS) Licenses – Optional** | **1 No** |
|  | **Grand Total** |  |

**L1 will be arrived on lowest quote received for supply, installation & implementation of required Hardware, SOC servers, deployment charges and other accessories for SOC solution and services on Total Packages i.e. sum (sno. 1 to sno. 12) as mentioned above.**

* Bidder has to quote basic price, applicable GST etc. in the item data column. Applicable GST can be selected from the dropdown box. In case any applicable GST are not available in the dropdown box, the same may be clearly mentioned along with the % in the #Bidders remarks#.
* Bidder has to quote for all items in SRM. Partial quote will not be considered.
* If BEML requires procuring additional 1000 EPS licenses in the future, the bidder should be able to supply the same as per the proposed rate in item no 13. Bidder should note that the cost shall be proportionate w. r. t. line item no 10. This line item no 13 is not calculated for arriving L1.If BEML requires procuring additional EPS licenses over and above additional 1000 EPS licenses in the future, the bidder should be able to supply the same on pro-rata basis.

**Technical bid will be considered subject to receipt of original DD for EMD / EMD Exemption Certificate/ Bid Guarantee & Integrity Pact.**

Price bid of only technically accepted/qualified offers will be opened subsequently.

Incomplete/invalid tenders will be rejected and no correspondence will be entertained in case of rejection.

1. **QUERY**

In case, if any clarifications are required for any topic related to the RFQ, the same may be submitted in writing, via e-mail to the designated Point of Contact through email address of CIO on or before 12**.09.2020**. All questions regarding this RFQ will be clarified during Pre-Bid meeting or subsequently after obtaining concurrence from the Management**.**

**Contact Name & Address:**

The following officer can be contacted for any clarifications and / or bid submission:

**Chief Information Officer**

BEML Limited, BEMLSoudha,

23/1, 4th Main, SR Nagar,

Bengaluru – 560027

Phone: 080-22963190/ 267

E-mail id: [ravib@cto.beml.co.in](mailto:ravib@cto.beml.co.in) /dgmerp@beml.co.in

copy to purchase@purchase.beml.co.in

In order to ensure a fair and open competition, BEML shall upload all queries and its clarifications, if any, in BEML website & CPP Portal.

1. **PRE-BID MEETING**

A Pre bid meeting will be conducted to clarify all the doubts with respect to the RFQ and scope of work. Interested vendors are requested to attend the pre-bid meeting scheduled at 11.00 **AM on 14.09.2020** at BEML Soudha, 23/1, 4th Main, SR Nagar, Bangalore-560027. Interested bidders shall confirm their participation well in advance before 13.09.2020. pre bid meeting will be conducted through **video conferencing**.

1. **PAYMENT TERMS:**

a) **Hardware**: 100% payment on 30th day for MSEs and for others on 60th day from thedate of receipt of Hardwares (item slno 1 to 6) at respective locations i.e. Corporate Office & Mysore Complex and acceptance by the respective BEML IT Department.  
  
b) **Software & Implementation**:100% payment on 30th day for MSEs and for others on 60th day after successful completion of scope of work i.e. supply & implementation (item slno 7,8,9 & 10) at respective locations i.e. Corporate Office & Mysore Complex and acceptance by the respective BEML IT Department.  
  
c) **Resources & AMC charges:** Payment will be made in arrears on completion of each quarter (every 3 months) of service duly certified by Corporate IT Department (item slno 11 & 12).

**Annexure - A**

**BID GUARANTEE FORMAT**

Ref:

To,

BEML LIMITED

BEML Soudha

No: 23/7, 4th Main, S.R. Nagar

Bangalore - 560027

Dear Sirs,

......................................................................................................................................................

In accordance with your ‘Tender Enquiry’ under your Tender No: …………...................dated

---------------------------M/s........................................................................................ herein after called the Bidder, with the following Directors on their Board of Directors / partners of the Firm.

1. 2.

3. 4.

5. 6.

7. 8.

9. 10.

Wish to participate in the said tender for ...............................................................................

…………………………………………………………………………………………………

.

……………………………………………………………………………………..................

As an irrevocable Bank Guarantee against Bid Guarantee amount of Rs……………………………......................................................................................(In words and figures) valid for ….. ………….. days from………………………………………….. is required to be submitted by the Bidder as a condition for participation in the said bid, which amount is liable to be forfeited by the BEML Limited (herein after called PURCHASER) (1) the withdrawal or revision of toe offer by the Bidder as a condition within the validity period. (2) Non-acceptance of the ‘Letter of Intent / Purchase Order’ by the bidder when issued within the validity period. (3) Failure to furnish the valid contract performance guarantee by the bidder within one month from the receipt of the Purchase Order and (4) on the happening of any contingencies mentioned in the bid documents.

We, the …………………………………………..Bank at.................................................

having our Head office at ……………………………………………..............................(Local address) Guarantee and undertake to pay immediately on first demand by BEML LIMITED, the amount of Rs......................................................................................................................

(in figure and words) without any reservation, protest, demur and recourse. Any such demand made by the Purchaser shall be conclusive and binding on the Bank irrespective of any dispute or difference raised by the purchaser.

The guarantee shall be irrevocable and shall remain valid up to .............................................. (This date shall be 60 days after the date for which the bid is valid). If any further extension of this guarantee is required the same shall be extended to such required period (not exceeding one year) on receiving instruction from M/s.………………………….. ...................................................................................... on whose behalf this guarantee is issued.

In witness whereof the Bank, through its authorized officer has set its hand and stamp on this …………………day of……………………………..at .........................................................

Witness (Signature)

WITNESS (Signature) ….

Name in (Block letters)

Designation ……………………………

(Staff No.) ……………………….

(Bank's common Seal)

Official address

Attorney as per power of Attorney No

Date:

**Annexure – B**

**(***To be executed on plain paper and applicable for all tenders of value ≥ Rs1Crores)*

**INTEGRITY PACT**

**Between**

**BEML Limited (BEML) hereinafter referred to as “The Principal”**

**and**

………………………….**hereinafter referred to as “The Bidder/Contractor”**

**Preamble**

The Principal intends to award, under laid down organizational procedures, contract/s for …………………………………….The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Principal will appoint an independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

**Section 1 – Commitments of the Principal**

1. The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:
2. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
3. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/ additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
4. The Principal will exclude from the process all known prejudiced persons.
5. If the principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or it there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

**Section 2 – Commitment of the Bidder(s)/ contractor(s)**

1. The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.
2. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal’s employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.
3. The Bidder(s)/ Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
4. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further, the Bidder(s) / Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or documents provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.
5. The Bidder(s)/ Contractor(s) of foreign origin shall disclose the name and address of the Agents/ Representatives in India, if any. Similarly, the Bidder(s)/ Contractor(s) of Indian Nationality shall furnish the name and address of the foreign Principals, if any. Further, as mentioned in the “Guidelines on Indian Agents of Foreign Suppliers” shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the “Guidelines on Indian Agents of Foreign Suppliers” is placed at placed at **Enclosure.**
6. The Bidder(s) / Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.
7. The Bidder(s)/Contactor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

**Section 3 – Disqualification from tender process and exclusion from future contracts**

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or any other form such as to put his reliability or creditability in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the “Guidelines on Banning of business dealings”.

**Section 4 – Compensation for Damages**

1. If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.
2. If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the contract value or the amount equivalent to Performance Bank Guarantee.

**Section 5 – Previous Transgression**

1. The Bidders declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti corruption approach or with any other Public Sector Enterprises in India that could justify his exclusion from the tender process.
2. If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in “Guidelines on Banning of business dealings”.

**Section 6 – Equal treatment of all Bidders /Contractors /Sub-contractors**

1. The Bidder(s)/ Contractor(s) undertaker(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact, and to submit it to the Principal before contract signing.
2. The Principal will enter into agreement with identical conditions as this one with all Bidders, Contractors and subcontractors.
3. The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

**Section 7 – Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)**

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or of the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer

**Section 8 – Independent External Monitor / Monitors**

1. The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the CMD, BEML.
3. The Bidder(s)/ Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s) / Subcontractor(s) with confidentiality.
4. The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The Monitor will submit a written report to the CMD, BEML, within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise submit proposals for correcting problematic situations.
7. If the Monitor has reported to the CMD, BEML, a substantiated suspicion of an offence under relevant IPC/PC Act, and the CMD, BEML has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
8. The word ‘**Monitor’** would include both singular and plural.

**Section 9 – Pact Duration**

This pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/ determined by CMD of BEML.

**Section 10 – Other provisions**

1. This agreement is subject to Indian Law. Place of performance and jurisdiction is the Corporate Office of the Principal, i.e. Bangalore.
2. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
4. Should one or several provisions of this agreement turn out to be invalid, the reminder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intensions.
5. In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the integrity pact will prevail.

---------------------------------------------------------- -------------------------------------------------------------------

(For & On behalf of the Principal) (For & On behalf of Bidder/Contractor)

(Office Seal) (Office Seal)

Place-------------------- Place--------------------

Date -------------------- Date --------------------

***Witness 1: Witness 1:***

*(Name & Address)* ------------------------------- *(Name & Address)* -------------------------------

------------------------------- -------------------------------

------------------------------- -------------------------------

------------------------------- -------------------------------

***Witness 1: Witness 1:***

*(Name & Address)* ------------------------------- *(Name & Address)* -------------------------------

------------------------------- -------------------------------

------------------------------- -------------------------------

------------------------------- -------------------------------

**Tender No: 6300034088 Date: 03.09.2020**

**Enclosure to Annexure –B**

**GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS**

1.0 There shall be compulsory registration of agents for all Global (Open) Tender and Limited Tender. An agent who is not registered with BEML LTD shall apply for registration in the prescribed **Application-Form** available on [*www.bemlindia.in*](http://www.bemlindia.in)

1.1 Registered agents will file an authenticated Photostat copy duly attested by a Notary Public/Original certificate of the principal confirming the agency agreement and giving the status being enjoyed by the agent and the commission/remuneration/salary/ retainer ship being paid by the principal to the agent before the placement of order by BEML LTD.

1.2 Wherever the Indian representatives have communicated on behalf of their principals and the foreign parties have stated that they are not paying any commission to the Indian agents, and the Indian representative is working on the basis of salary or as retainer, a written declaration to this effect should be submitted by the party (i.e. Principal) before finalizing the order.

**2.0 DISCLOSURE OF PARTICULARS OF AGENTS/ REPRESENTATIVES IN INDIA, IF ANY:**

2.1 Bidders of Foreign nationality shall furnish the following details in their offer:

2.1.1 The name and address of the agents/representatives in India, if any and the extent of authorization and authority given to commit the Principals. In case the agent/representative be a foreign Company, it shall be confirmed whether it is real substantial Company and details of the same shall be furnished.

2.1.2 The amount of commission/remuneration included in the quoted price(s) for such agents/ representatives in India.

2.1.3 Confirmation of the bidder that the commission/ remuneration if any, payable to his agents/ representatives in India, may be paid by BEML LTD in Indian Rupees only.

2.2 Bidders of Indian Nationality shall furnish the following details in their offers:

2.2.1 The name and address of the foreign principals indicating their nationality as well as their status, i.e, whether manufacturer or agents of manufacturer holding the Letter of Authority of the Principal specifically authorizing the agent to make an offer in India in response to tender either directly or through the agents/representatives.

2.2.2 The amount of commission/remuneration included in the price (s) quoted by the Bidder for himself.

2.2.3 Confirmation of the foreign principals of the Bidder that the commission/remuneration, if any, reserved for the Bidder in the quoted price (s), may be paid by BEML LTD in India in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Stores and Spares in case of operation items.

2.3 In either case, in the event of contract materializing, the terms of payment will provide for payment of the commission /remuneration, if any payable to the agents/representatives in India in Indian Rupees on expiry of 90 days after the discharge of the obligations under the contract.

2.4 Failure to furnish correct and detailed information as called for in paragraph-2.0 above will render the concerned tender liable to rejection or in the event of a contract materializing, the same liable to termination by BEML LTD. Besides this there would be a penalty of banning business dealings with BEML LTD or damage or payment of a named sum.

--------x-------

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure - C**

**DETAILS TO BE FILLED/ UPLOADED BY THE PARTICIPATING FIRM**

|  |  |  |
| --- | --- | --- |
| **Sl. No.** | **Description** | **Details to be filled/uploaded** |
| 1 | Name of the Firm& Postal address for correspondence (With name of the Contact Person) with telephone number, fax and email id |  |
| 2 | Bank Details like Bank account numbers & IFSC code with Banker’s Name, Address & Contact No.: | Bank account numbers :-  IFSC Code:  Banker’s Name :-  Branch Name:  Address :-  Contact Number :- |

I / we hereby certify that all the information given above is factual.

*Signature with date of Authorized signatory*

*Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Firm’s Seal:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure - D**

**Technical Specifications**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Technical Specifications** | **Compliance (Yes)** |
| **A.** | **SIEM Security Incident and Event Management Tool ( Required)** | |
|  | The proposed appliance should be SIEM OEM appliance. The SIEM OEM should have end to end support for this appliance. |  |
|  | The proposed product should be able to handle minimum of 3,000 sustained EPS which is scalable upto 15,000 EPS. All hardware should be sized on minimum 15,000 EPS. In any given situation the SEIM solution should not drop any events during log collection. |  |
|  | The peak EPS that the proposed solution can address without any additional license, server or appliance should be minimum twice than the sustained EPS proposed |  |
|  | The proposed solution should have option to store Raw Logs and associated normalized events should be retained for 3 months on online media. The online media should query and reports may be executed against this 1 year of logs on Backup Media and 4 years of archival. The proposed solution should mandatorily store normalized logs for specified time duration mentioned. |  |
|  | High availability would be required at the log-collection layer in DC is mandatory & DR is optional |  |
|  | The log storage for retention of online data (3 months) should be available at DC& DR. |  |
|  | If the primary analysis/correlation engine is not functional all correlation activity should be possible from secondary site as well. |  |
|  | If the primary analysis/correlation engine is not functional all correlation activity should be possible from secondary site as well. |  |
|  | The Solution should have separate log collection layer, Log Management layer and correlation layer. Log Correlation layer should not pull logs from log management to correlate as this impacts performance. |  |
|  | All the communication between the various components of the SIEM solution should be secured. |  |
|  | The solution should detect and alert an interruption in the log collection process. |  |
|  | The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in 15 minutes then generate an alert. |  |
|  | All business applications would be integrated in subsequent phases using custom parsers that could fetch the logs using any of the protocols like file reader, syslog or ODBC connections |  |
|  | Proposed SIEM solution should have out of the box content for MITRE ATT&CK Framework. Default rules should be mapped with MITRE ATT&CK Techniques. |  |
|  | The system shall allow custom dashboards for real-time alerts, reports etc. |  |
|  | The system should have interface to monitor health of the various components of solution and provide details like CPU usage, interface usage, disk status etc |  |
|  | OEM should support the solution for 6yrs from the date of completion of implementation of the solution. |  |
|  | The solution must map and segregate assets as per asset classification data feed into SIEM solution. |  |
|  | Proposed SIEM solution should have inbuilt ticketing system. Which should include automated and manual incident creation, updation, escalation etc. |  |
|  | The proposed SIEM solution should have built-in use cases along with open source Threat Intelligence Platform (TIP) integration capability. |  |
|  | SIEM tool should be running 24\*7\*365 for monitoring of the devices/ servers |  |
| **B.** | **SOC Case Management, Incident Response and End Point Detection ( Required)** | |
|  | Solution Should have curated threat intelligence from dark web, deep web and surface web threat feeds integration. |  |
|  | Possibility to enter IOCs manually by analysts |  |
|  | Data visualization capabilities to determine analyst efficacy and overall threat landscape |  |
|  | Integration with MITRE, NIST and Cyber Kill Chain frameworks |  |
|  | Should have a functionality for case checklist- list of steps tailored for a particular type of alert |  |
|  | Internal knowledge base to create a list of blacklisted IPs, Vulnerable IPs etc. |  |
|  | Role based access for case management. |  |
|  | Support for performing bulk action |  |
|  | Periodic reporting capabilities |  |
|  | The Solution should have a dedicated endpoint threat detection agent which can run scan(s) to identify and collect suspicious running Processes, Autoruns, Files, Drivers, Libraries, File, Systemd, Cron, Initd, daemon and System Information on an Windows / Linux / MacOS endpoint. This agent should be separate from the AntiVirus (AV) solution and not from the same OEM to ensure that threats which are missed by AV are detected by endpoint agent. |  |

Signature with date of Authorized signatory

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firm’s Seal:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure –E**

**UNDERTAKING**

To:

The General Manager (Corporate Materials),

M/s. BEML LTD

Bangalore-27

Dear Sir,

Having examined the Bid Invitation No. 6300034088 dated 03.09.2020 the receipt of which is hereby duly acknowledged, we, the undersigned, hereby confirming that we read, understood and accepting all the terms & conditions available in the tender. Further, we indicate that upon selection, we will execute the assignment as per the tender terms and conditions.

Signature with date of Authorized signatory

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firm’s Seal:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure - F**

**DESIRABLE TECHNICAL SPECIFICATIONS OF SIEM & SOC**

| **Sr. No.** | **Technical Specifications** | **Compliance (Yes/No)** |
| --- | --- | --- |
| **A**. | **Security Incident and Event Management Tool(Desirable)** | |
|  | 1 Minimum specification of each layer to be as below:  **Log Collection: - Qty 2 Nos.** - 1 No in DC, 1 No in DR  16-core Intel Xeon, 2.1 GHz CPU  64 GB RAM  4 TB HDD (usable) RAID5  **Log Management: - Qty 2 No.** - 1 No in DC, 1 No in DR  24-core Intel Xeon, 2.3 GHz CPU  192 GB RAM  24 TB HDD (usable) RAID5  **Log Correlation: - Qty 1 No.**  32-core Intel Xeon, 2.1 GHz CPU  256 GB RAM  5 TB HDD (usable) - RAID10 1 No in DC.  **EDR Management server:- Qty 1 No.**  4 Core, 16GB RAM, 500 GB HDD  Windows 2019, MS SQL 2016 SP1  **Storage for Archive:** - **- Qty 1 No.**  55 TB – 10k RPM SATA/SAS/FC |  |
|  | In case if correlation layer is not available then log management layer should be able to do forensics on logs, reporting, basic dashboards etc. at the time of incident. |  |
|  | Support for the Integration of Security Logs from the following devices/application systems but not limited to: Operating Systems (Windows 2003, 2008, 2012, 2016) Database(Oracle, MYSQL, SQL etc.)Anti-Virus solution (Symantec) Proxy logs(Barracuda)Firewall logs, Network Devices(Routers, switches etc.)Security Devices (NGFW, IPS, Anti APT, DDOS etc.)Tools(VA Tools) Directories (AD, LDAP etc.)Network flows (i.e. Netflow, J- Flow.) Logs from Application infrastructure (Web Servers, App Servers, Mail Server, Middleware etc) Logs from Application (in house applications, Internet Portal, P&GS, Mail application-Mdaemon etc.,)  This is an indicative list and the product should be capable of integrating the logs for other systems/OS/devices too, which may not be included in the list and may be deployed by us at a later date. |  |
|  | The solution must support both agent and agentless industry log collection methods (syslog,WMI, JDBC, SNMP, Checkpoint LEA, Pull from file etc.) |  |
|  | All logs should be automatically categorized into categories like firewall, IPS, operating system etc |  |
|  | The solution must have the capability to analyze and process large unstructured and structured data in a faster way. |  |
|  | The solution should support the collection and normalization of custom log data (e.g. custom application logs data, etc.) Log normalization, categorization should be done on log collection layer. Log filtering functionality while forwarding logs from collection and log management to correlation layer should be available. |  |
|  | The users have the ability to write their own device support for custom log formats. |  |
|  | The proposed solution should parse flat files collected from other systems. |  |
|  | If collectors are used to relay log data, the solution should continue to collect and store log data during a communication interruption for a minimum of two days (e.g. WAN link has gone down)? |  |
|  | The solution should guard against tampering during log collection and support chain of custody and non-repudiation efforts. For example: every event after normalization should have additional time stamp added collection layer, log management layer/Correlation layer. |  |
|  | The SIEM Solution must have central UI for policy configurations, Rule creation & raw log search |  |
|  | The SIEM Solution search interface must provide support for simple Boolean-style search patterns as well as complex regular expressions and free text search. |  |
|  | The SIEM solution search performance must be capable of searching through millions of unstructured (raw) log messages within few minutes. |  |
|  | The proposed solution should support external storage integration for log storage and archival. |  |
|  | The SIEM solution should ensure the integrity of raw log data once it's been archived. |  |
|  | The system should be able to integrate new data sources into existing collectors, without disruption and loss of data to the ongoing data collection. |  |
|  | Event transport must be able to send to multiple destinations for HA purposes. Each transport path must be independently configurable from the other. Should support forwarding up to 4 destinations minimum. |  |
|  | The solution should provide SDK to build custom parsers for integrating proprietary/custom applications. Bidder has to consider atleast 10 custom parsers scope as per the device/application list shared in the RFP. |  |
|  | For assets not natively supported, the SIEM solution should provide the collection of events through customization of connectors or similar integration; Must support event collection using at least the following industry standards: syslog, OPSEC, WMI, RDEP, EDDS, ODBC, JDBC, FTP, SCP, HTTP, file text, CSV and XML file. |  |
|  | The product must provide some mechanism that guarantees delivery of events to the log management system and that no events will get lost if the log management system is unavailable. i.e., Logs should be cached locally on the collection layer. |  |
|  | The solution should support RADIUS, Active Directory, LDAP for Authentication |  |
|  | The system shall compress on-line data as well as offline (archived) data to minimize storage requirements. |  |
|  | Sensitive Fields in the logs should de-identifed so that SOC analyst should not be able to see sensitive data. Only authorized users should be able to re-identify the sensitive data. |  |
|  | Every log event should be given a unique event id so that event can be tracked across multiple layers of SIEM. |  |
|  | The solution should be able to correlate on any fields in the event. |  |
|  | The solution should provide out of box rules for alerting on threats found in log or network data (but not limited to)- E.g. - failed logins, account changes, expirations, port scans, suspicious file names, default usernames, default passwords, security tools, AV signature updates, successful authentications, bandwidth by IP, email senders, failed privilege escalations, VPN failed logins, group management system configuration changes, traffic to non- standard ports, URL blocked, accounts deleted, accounts disabled, top intrusions etc. |  |
|  | The solution should allow creating correlation rules on desired meta report. |  |
|  | The solution should support the following types of correlation conditions on log data (not limited to)- 1) Event following by another event  2) ON OFF conditions. E.g. Event followed by absence of second event.  3) Grouping, aggregations, sort, filter, merge etc.  4) Alert suppression,  5) Avg, count, min, max  6) Regex Support  Should also support nested correlation rules. For example, One rule should provide an input to another rule. |  |
|  | The solution should allow creating cross device correlation rules that can take multiple scenarios like and create alert based on scenarios like (not limited to)- 1) Login on VPN followed by multiple failed logins to windows Where source IP(from VPN) is not in India 2) Multiple Failed logins from users where user has not changed the account password in last 2 days. |  |
|  | The solution should also support historical correlation. Capability search for matching historical data using a new correlation rule |  |
|  | The solution must provide alerting based upon established policy. (e.g., IM traffic is not allowed.) |  |
|  | The solution must support weighted alerts to allow for prioritization. Weights must be assignable based on multiple characteristics such as asset type, protocol, application, etc. |  |
|  | The solution must support the ability to correlate against 3rd party vulnerability scan results as well as internal scan reports. Please provide the list of out of the box VA vendors supported and describe how to integrate unsupported vendors. |  |
|  | The solution must provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base servers) to minimize false positives associated with poor asset classification. |  |
|  | The solution must provide the ability to model incoming event data into logical groups such as domains, networks, applications, criticality of target devices, etc. This data modelling should then be available to assist in filtering and logically segregating data from view. |  |
|  | The solution must provide a complete audit trail and accountability during the incident handling or forensic investigations. |  |
|  | The product must be capable of maintaining event receipt time for all events. This allows integrity for forensic analysis of logs to determine the original time on the event source and what the system time was for each vendor component processing the event. Timestamp should be added at each layer of SIEM; like collector should add a time stamp, log management should add a time stamp and correlation engine should add a time stamp. |  |
|  | The SIEM Solution should provide a formula of threat which should be customized to allow increasing or decreasing the level of risk with the following types of correlation (not limited to): A. Geo Location Based Correlation  B. Historical Based Correlation  C. Vulnerability Based Correlation |  |
|  | The SIEM Solution should have a module that can also allow segregation of duties management, real-time correlation, historical correlation, reporting and access interface between one or more appliances, allowing more efficient use of the overall performance of the devices. |  |
|  | The SIEM Solution must possess module that allows risk analysis activities in the network infrastructure. |  |
|  | The system should have the capability to automatically represent detected attacks in graphical view in real time. |  |
|  | Physical vs. Logical Correlation: The system should be able to correlate information based on physical locations and logical actions. |  |
|  | All out of box parsers and toolset to prepare or modify existing parsers to collect any type of log or add additional contextual information should be made available to the operations team and adequate training imparted for them to work independently on these modifications and enhancements. |  |
|  | It should be possible to correlate and report on all logs that are collected by the system. Analysis should be possible both on real time logs as well as historical logs. |  |
|  | Normalization of events collected should be performed on all events received by the system proposed so as to ensure that all logs are queriable and drillable. Also, normalization should happen at collection layer or collectors. |  |
|  | The SIEM solution must provide the ability to limit bandwidth used for transmitting event data from remote sites. |  |
|  | Normalization of logs should allow recording of any environmental/ contextual data related to event but not available within the event data itself – e.g. location data of source system, risk value of source etc. |  |
|  | It should be possible to add any real time contextual information/ situational awareness data into the normalized data for long term storage |  |
|  | All logs that are collected should be studied for completeness of information required/ reporting/ analysis and requisite data enhancement/ normalization should be performed to meet the reporting/analysis needs. |  |
|  | The solution should allow creating reports from the rules provided by vendor or created by administrator (for both the online as well as the archived data) |  |
|  | The reports should be available for the following (not limited to):  a). Payment Card Industry (PCI) b). ISO  (Please specify all such compliance reports and indicate the numbers against each report category.) |  |
|  | Compliance and security relevant reports should be available out of the box or necessary license should be factored. The solution must be able to customize the out of the box reports as well. (please specify no. of reports available in Remarks column) |  |
|  | The solution should provide creation and customization of reports for any new Management and Business requirements. |  |
|  | The solution should provide both tabular and graphical reports |  |
|  | The solution should allow adding custom content to the report like headers, footers, table of content, notes etc. |  |
|  | The system should allow scheduling reports and send it via email. |  |
|  | The system should provide a calendar view. Clicking on a date should show all reports generated on the selected date |  |
|  | Reports should be available in pdf, csv, word and html format. |  |
|  | The system must allow free text search features such as Google search. |  |
|  | The solution must provide a flexible dashboard with chart and summary displays for a complete view of real-time captured data. |  |
|  | The solution must be able to schedule reports and also provide the flexibility to generate on-demand reports. |  |
|  | The solution must provide fully customizable queries and report library to define report and alert combinations. |  |
|  | Create chart rule, schedule and view dynamic chart in time and summary series format. |  |
|  | The solution must support the automated distribution of reports. |  |
|  | The solution must support the ability to centrally deliver asset reports. |  |
|  | The solution should allow creating custom log source lists to provide a direct mapping for log sources that fall in-scope for regulatory compliance |  |
|  | The solution must provide ability to send notification of correlated alerts via well-defined methods (i.e. SNMP trap, email, SMS etc.)? Please describe how your solution meets this requirement. |  |
|  | The system shall provide a report designer that allows users to customize the appearance of the report such as adding of organization logo in the report, modifying the graphs, tables, grouping, sorting, etc. |  |
|  | The report creation process should have no impact the log collection process |  |
|  | Please provide the list with sample reports that can be generated by the SIEM. Also mention the detailed list of use case reports that can be configured on the solution. |  |
|  | Proposed SIEM solution should have data science engine which enables analysts to do predictive analysis in reports. |  |
|  | The system should allow centralized management and reporting for various components from a single web-based user interface. |  |
|  | The system should allow centralized system updates for application |  |
|  | End user & Admin access with required licenses should be included for unlimited users. |  |
|  | The system should audit all changes made to all the components of the SIEM system. |  |
|  | The solution should provide GUI Management capability. |  |
|  | The administrator must be able to define role-based access to various functional areas of the solution and restrict users’ role including, but not limited to, administration, reporting, event filtering, correlation, and/or dashboard viewing. |  |
|  | The data collected from the receiver should be forwarded in an encrypted manner to SIEM log storage |  |
|  | The system shall provide the function to update the product version or components such as reports packages. This process shall occur seamlessly and transparently |  |
|  | The system should be able to report on its own system health and availability. Notifications through email shall be sent out if the system health or availability is failing |  |
|  | The solution should support configurable data retention policy. |  |
|  | The system shall support centrally controlled upgrade of log collectors/agents |  |
|  | The solution must ensure all distributed system components continue to operate when any other part of the system fails or loses connectivity. (i.e., if management console goes off-line all separate collectors still continue to capture logs). |  |
|  | The solution must have an automated backup/recovery process. |  |
|  | The solution must provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system. |  |
|  | The solution should allow to create incident reports based on (not restricted to) owners, status, application, Business Process, Business units, locations, asset groups, Business owners etc. |  |
|  | The System should provide capability to consolidate the Incidents, VA scanning results, other policy violations, Configuration Compliance Scan results, Penetration testing results and Patch management tool result and link those results directly to physical assets/ Devices which in turn should be mapped with Applications, Business processes, facilities if applicable. The system should relate threats to the assets they affect, enabling the prioritization of patches or workarounds based on asset criticality. Capability should also include integration of email advisories and RSS feeds. |  |
|  | The system should support event log enrichment with asset classification by asset owners, based on rating attributes (but not limited to)  - Criticality rating  - Confidentiality rating  - Integrity rating  - Availability rating |  |
|  | The system should provide capability to capture incidents of any type, including SIEM, Physical Security, unauthorized access, etc.) and cyber incidents (e.g. IT Security, malware, phishing, etc.). |  |
|  | The solution must provide a mechanism to create single dashboard to capture all relevant aspects of a security incidents. This should include relevant events, network activity data, correlated alerts, vulnerability data, etc. |  |
|  | Solution must be able to integrate with third- party Help Desk systems such as BMC Remedy/CA/IBM/HP etc. Integration must support at a minimum: automated and manual incident creation, updating of existing incident, synchronization of incident closure |  |
|  | The solution should allow the user to retrieve the system logs for diagnostic purposes or to send such logs to the Support department for troubleshooting. |  |
|  | The solution should have an overall view of the tasks that have been scheduled. An example of a scheduled task could be a Daily Report, automated backup etc. Such overall view will allow the user to have a visibility on the number of background tasks running on the system. |  |
|  | The sign-off for the overall solution would be provided after integration of all devices and availability of reports as per our requirements. |  |
| **B.** | **SOC Case Management, Incident Response and Endpoint Detection Response ( Required)** | |
|  | The proposed SIEM solution should have built-in use cases along with open source Threat Intelligence Platform (TIP) integration capability. The proposed SIEM solution tool should also have OOD integration with SOAR functionalities and the bidder need to supply and implement the SOAR solution from the same OEM. |  |
|  | AI and ML capabilities to provide qualitative and quantitative assistance to analysts |  |
|  | A full packet capture software should be provided with 256 Mbps  line rate with multiple ingress interfaces for capturing from multiple  network interfaces. |  |
|  | The solution Should be able to provide complete packet-by-packet  details pertaining to one or more session of interest including Session  replay, page reconstruction, image views, artefact & raw packet and  object extractions. |  |
|  | The Solution should have endpoint threat detection agent supporting all major operating systems like Windows etc., |  |
|  | There should be a single dashboard with integrated and native correlation between logs and EDR solution |  |

Signature with date of Authorized signatory

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firm’s Seal:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure - G**

**SPECIFICATIONS FOR LED DISPLAY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No** | **Description** | **Specification** | **Specification offered by the firm**  **( To be filled).** |
| 1 | Make | Any Reputed Make  **No China Make** |  |
| 2 | Diagonal Size | 55" |  |
| 3 | Resolution | 3840\*2160 (4K UHD) |  |
| 4 | Response Time(G-to-G) | 8ms |  |
| 5 | Viewing Angle Degree | 178 x 178 |  |
| 6 | Operation Hour | 16/7 |  |
| 7 | Connectivity | HDMI / DVI / RS232 / USB / RJ45 |  |
| 8 | Brightness | 350 nits or better |  |
| 9 | External Control | RS232C(in/out) thru stereo jack, RJ45 |  |
| 10 | Operating Hours | 24x7 |  |

Signature with date of Authorized signatory

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firm’s Seal:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure - H**

**UNDERTAKING**

This is to certify that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Name of the Firm) has not been banned / black listed / debarred from Trade by any Central /State Govt. Dept. / Autonomous Institution / PSUs in India at the time of bidding.

I / we hereby certify that all the information given above is factual.

Signature with date of Authorized signatory

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firm’s Seal:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure - I**

**Special Conditions arising out of implementation of GST**

**(Which is to be signed and submitted along with the offer)**

**GST Terms & Conditions**

1. The Supplier is required to comply with all the applicable provisions of the GST Laws/Rules/Notifications/Circulars and to furnish required documents/details within the prescribed time limit to enable BEML to claim the benefits of GST Input Tax Credit or any other benefit.
2. The Supplier is required to furnish proper Invoice/Supplementary Invoice/Debit Note/Credit Note in the form and manner prescribed under GST Laws/Rules/Notifications/Circulars containing all the particulars mentioned therein and within the prescribed time limit as per prevailing GST Laws/Rules/Notifications/Circulars. In case of non-compliance by the Supplier, BEML shall not make any payment towards GST against such invoice until it is complied with within the timeline prescribed under GST Laws/Rules/Notifications/Circulars, and also subject to BEML being in a position to avail GST Input Tax Credit as per applicable GST Laws/Rules/Notifications/Circulars.
3. In case of discrepancy in the data uploaded by the Supplier in the GSTN portal or incase of any shortages or rejection in the supply, BEML will notify the Supplier of the same. Supplier has to rectify the data discrepancy in the GSTN portal or issue Credit note (details to be uploaded in GSTN portal) for the shortages or rejections in the supplies, within the prescribed time limit to enable BEML to avail GST Input Tax Credit.
4. In case, the availment of GST Input Tax Credit by BEML is delayed for any reason other than those attributable to BEML, interest at applicable rate as prescribed under GST Laws/Rules/Notifications/Circulars for such delays shall be recovered from the Supplier.
5. In case Supplier delays declaring such invoice in his GST Return and GST Input Tax Credit availed by BEML is denied or reversed subsequently as per GST Laws/Rules/Notifications/Circulars, GST amount paid by BEML towards such reversal as per GST Laws/Rules/Notifications/Circulars shall be recoverable from Supplier along with applicable interest.
6. If BEML has not paid/short paid to the Supplier for any invoices within the time limit prescribed under GST Laws/Rules/Notifications/Circulars due to non-compliance of GST Laws/Rules/Notifications/Circulars by Supplier or any other reason attributable to Supplier and leads to any GST Input Tax Credit reversal by BEML, any losses/expenses/cost/penalty, etc incurred by BEML shall be recoverable from the Supplier.
7. Wherever applicable, BEML will have the right to deduct “Tax Deducted at Source” at the rate prescribed under the GST Laws/Rules/Notifications/Circulars and to remit the same to the Government.
8. In case of supplies made under Reverse Charge Mechanism, the Supplier needs to comply with the provisions under the GST Laws/Rules/Notifications/Circulars in terms of supply of Goods/Services and raising of invoice, so as to enable BEML to remit applicable GST to Govt., within the prescribed time limit and avail GST Input Tax Credit on the same. If the Supplier fails to comply with the above and as a result if BEML incurs any losses/expenses/cost/penalty, BEML shall be entitled to recover the same from the Supplier. Further the Supplier has to mention that “the liability of payment of GST amounting to Rs ……. is on the Recipient of Service” in the invoice raised on BEML.
9. The Supplier is required to comply with the E-Way Bill Provisions under GST Laws/Rules/Notifications/Circulars. If the Supplier fails to comply with the said provisions and as a result if BEML incurs any losses/expenses/cost/penalty, BEML shall be entitled to recover the same from the Supplier.
10. In case of materials/goods issued to Supplier for Job Work, the Job Work Supplier is required to return the goods within the time limit prescribed in the Purchase Order. If the Job Work Supplier fails to return the goods as above, BEML will be entitled to raise a GST Supply Invoice on the Job Worker Supplier with applicable interest as per the provisions of GST Laws/Rules/Notifications/Circulars. In such cases, BEML will be entitled to recover all such GST/interest on GST /losses/expenses/cost/penalty, etc. incurred by BEML along with interest from the Job Work Supplier. Further in such cases where the GST invoice has been raised by BEML, on return of such goods after the prescribed time limit, the Job Work Supplier needs to return the same under GST invoice.
11. GST portion of the invoice shall be released only upon the Supplier declaring such invoice in his GST Return and payment of GST thereof to appropriate government and satisfying all the conditions mentioned above. However, in case the Supplier wishes to obtain the payment of GST portion also along with the payment of the base value of the invoice, Supplier has the option to submit Bank Guarantee of an amount equivalent to the GST portion of the invoice plus 3 months’ interest at prevailing rate of interest under GST Laws/Rules/Notifications/Circulars as applicable in case of reversal of GST Input Tax Credit. Such Bank Guarantee shall be valid till 30th September of the next financial year or filing of GST Annual Return by Supplier/Vendor (for which such invoice pertains to), whichever is earlier. BEML will release Bank Guarantee only when the Supplier declaring such invoice in his GST Return and remittance of GST thereon to the Govt. In case the Supplier fails to fulfill the required conditions resulting in BEML not been able to avail GST Input Tax Credit Bank Guarantee shall be encashed and such GST amount along with interest and any other cost/loss incurred by BEML shall be recoverable from Supplier.
12. The Supplier have the option to give one Bank Guarantee of appropriate value after considering his estimated value of GST involved in invoices raised on BEML instead of Bank Guarantee for each Contract/Invoice. In case of payment through LC, suitable provisions/clause will be inserted while opening LC to ensure compliances of above conditions. However, if at any point of time value of such Bank Guarantee falls short of GST plus interest thereof, Supplier will have to either furnish Bank Guarantee for Differential value or such shortfall value of Bank Guarantee vis-à-vis GST plus interest thereof shall be withheld till Suppliers fulfils its obligations specified under above clauses.
13. BEML will be entitled to recover all losses/expenses/cost/penalty, etc. incurred by BEML along with applicable interest from the Supplier due to reasons other than those attributable to BEML.
14. If the Supplier is a Composition/Unregistered Dealer, the Supplier needs to comply with the provisions under the GST Laws/Rules/Notifications/Circulars in terms of supply of Goods/Service and raising of invoice. In case, the Supplier fails to comply with the above and as a result if BEML incurs any losses/expenses/cost/penalty, BEML shall be entitled to recover the same from the Supplier along with applicable interest.

Place:

Date:

for M/s…………………..

Signature

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure - J**

**BIDDER HAS TO UPLOAD THE FOLLOWING COMPLIANCE SHEET AS PART OF THE TECHNICAL BID.**

| **Sl No** | **Criteria Details** | **Documents required to be uploaded in Collaboration folder of SRM system** | **Compliance sheet**  **(Yes / No)** |
| --- | --- | --- | --- |
| **MANDATORY** | | |  |
|  | Brief Details about the Firm | Please upload filled-in format as per **Annexure - C.** |  |
|  | The Bidder should be authorized / certified partner of the OEM. The Bidder must be in position to provide support / maintenance / upgradation during the entire period of contract. | Manufacturer Authorization Form (MAF) from OEM to be uploaded |  |
|  | The Bidder should have experience in supply, implementation, support and managed services of captive SOC with SIEM for any PSU / BFSI /Government / Enterprise customers in India. SOC solution with SIEM **(mandatory)** and should have at least 2 out of the following components apart from SIEM like Firewall, AAA (Authentication), WAF, DAM, PIM, NBA, Anti-APT solutions/Anti-Phishing, DLP, MDM, Anti-DDoS, NAC, and Vulnerability Management in the last 5 years  a. Three similar completed works costing not less than **Rs. 1.60 Crores**  Or  b. Two similar completed works costing not less than **Rs. 2 Crores**  Or  c. One similar completed works costing not less than **Rs. 3.20 Crores** | (PO / Work Order Copy related to establishment of SOC along with Completion certificate from the customer) or (PO Copy/Work Order related to establishment of SOC along with proof for completion of the work from the customer like invoice and payment details to the bank clearly mentioning the invoice details with reference to the PO). |  |
| **MANDATORY** | | |  |
|  | The Bidder should be ISO 9000 / 9001, or ISO/IEC 27001 certified, with certifications valid at the time of bid submission. | Documentary proof i.e. photocopies of certificates to be uploaded |  |
|  | Technical Specification of SIEM & SOC compliance sheet | Please upload the filled, signed & sealed technical Specification sheet as per **Annexure - D** |  |
|  | An Undertaking has to be submitted by the bidders stating that they have read, understood and agreeing to all tender terms and conditions. | Undertaking document as per **Annexure – E** to be uploaded in the collaboration folder. |  |
| **NON MANDATORY** | | |  |
|  | Average annual financial turnover during the last three years, ending 31st March of the previous financial year (i.e. 2017-18,2018-19 & 2019-20) should be minimum **Rs. XX Crores** | 2017-18 Rs.  2018-19 Rs.  2019-20 Rs.  Copies of audited balance sheet (indicating turnover) for last three years shall be uploaded in the collaboration folder.  **Note:** If the audited balance sheet for the FY 2018-19 is under audit, then provisional balance sheet to be provided otherwise the average annual turnover during the previous three years shall be considered for evaluation i.e. 2017-18, 2018-19, 2019-20. |  |
|  | The bidder should be a registered corporate in India registered under the Companies Act, 1956 or a company/statutory body owned by Central / State Government. | Certificate of Incorporation |  |
|  | Desirable Technical Specifications of SIEM | Please upload the filled, signed & sealed technical Specification sheet as per **Annexure - F** |  |
| **NON MANDATORY** | | |  |
|  | Technical specification for Display Unit | Please upload the filled, signed & sealed technical Specification sheet as per **Annexure - G** |  |
|  | Bidder/OEM should have their own SOC located in India | Self-Certificate with address |  |
|  | The bidder should have minimum 25 skilled staff with professional certifications like PMP/ CISSP / CEH/CCSP/CCNA/JNCIA/ISMS Auditor/CRE or Security OEM trained for SIEM, out of which at least 2 resources should be deputed for BEMLs SOC project | List of skilled staff with their Technical Qualifications and Self-Certification for the same to be uploaded |  |
|  | The bidder/OEM must possess all valid certificates as mentioned below and should upload copies of the same:   * + - * 1. PAN Number         2. GST Registration details/ Certificate | Please upload scanned copies of   1. PAN Number 2. GST Registration details/ Certificate |  |
|  | The vendor should not have been blacklisted by any government/ PSU/Reputed Listed company for corrupt or fraudulent practices or non-delivery, non-performance. | Undertaking document as per **Annexure – H** to be uploaded in the collaboration folder. |  |
|  | Special Conditions arising out of implementation of GST Tax Indemnity clause | **Annexure – I** to be signed and uploaded in the collaboration folder. |  |
|  | Bidder has to upload compliance sheet as part of the technical bid. | Please upload **Annexure – J** |  |

Signature with date of Authorized signatory

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Firm’s Seal:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tender No: 6300034088 Date: 03.09.2020**

**Annexure - K**

CONFIDENTIALITY AGREEMENT

This CONFIDENTIALITY AGREEMENT (the “Agreement”) is made and entered into on this \_\_\_\_\_ day of <Month> 2020 (the “Effective Date”), by and between **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** and incorporated under The Companies Act, 1956, having its registered office at **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** (hereinafter referred to as “**\_\_\_\_\_\_\_\_**”, which expression shall, unless it be repugnant or contrary to the context or meaning thereof, mean and include its, successors and permitted assigns) of the ONE PART AND **BEML LIMITED**, Central Public Sector Undertaking, under the administrative control of Ministry of Defence, Department of Defence Production, Government of India and a Company incorporated under the Companies Act, 1956, having its Corporate Office at **‘BEML SOUDHA’, 23/1, 4th MAIN, SAMPANGI RAMA NAGAR, BENGALURU 560027, KARNATAKA** (hereinafter referred to as “**BEML**” which expression shall, unless it be repugnant to the context or meaning thereof, mean and include its successors and permitted assigns), of the OTHER PART:

\_\_\_\_\_\_\_ and BEML shall hereinafter jointly be referred to as “Parties” and individually as “Party”.

WHEREAS:

\_\_\_\_\_\_\_\_\_\_\_ is engaged in the business of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

BEML is multi-technology heavy engineering Industry engaged in the business of design, development and manufacture of a variety of Earthmoving, Railways, Defence Equipments, Diesel Engines, Hydraulic & Power line aggregates and also providing services in the areas of engineering, design & development and trading, etc.

BEML issued a Purchase Order No. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_** to \_\_\_\_\_\_\_\_\_\_ for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (hereinafter referred to as **“the Purpose”.**

BEML may disclose, transmit and/or exchange certain “confidential information” as described herein to \_\_\_\_\_\_\_\_\_\_ for the purpose and \_\_\_\_\_\_\_\_\_ recognises that careful protection and non-disclosure of the Confidential Information is of vital importance and responsibility of \_\_\_\_\_\_\_\_\_\_.

NOW THIS AGREEMENT WITNESSETH:

**1. Interpretation:**

In this Agreement “**Confidential Information**” means all or any information or which is or has been disclosed to \_\_\_\_\_\_\_\_\_\_ (the “Recipient Party”) by BEML (the “Disclosing Party”), or come into the knowledge of \_\_\_\_\_\_\_\_\_\_ during the execution of the Purpose including but not limited to, financial, accounting ,past, current and future customer information, proprietary, technical, personnel, marketing, pricing, sales and/or commercial information as well as ideas, concepts, designs and inventions, embedded hardware design, data and information, computer source and object code and computer programming techniques; algorithms, software programs, program schedule, visual demonstrations, photographs, manuscripts, texts, video recordings, formulations, equipment or apparatus, oral discussions and all record bearing media containing or disclosing such information which shall interalia include letters, notes, briefs, technologies, notings, drawings, materials, and all other information pertains to the Disclosing Party which has come into the possession or knowledge of the Receiving Party. Confidential Information does not include information which:

1. is publicly available at the time of its disclosure; or
2. becomes publicly available following disclosure; or
3. is already known to or was in the possession of Recipient Party prior to disclosure under this Agreement; or
4. is disclosed to the Recipient Party by a third party, which party is not bound by any obligation of confidentiality; or
5. is or has been independently developed by the Recipient Party without using the Confidential Information;
6. is disclosed with the prior consent of the Disclosing Party.

**2. Confidentiality:**

* 1. The Recipient Party agrees to regard, preserve and keep as secret and confidential all confidential information of the Disclosing Party or its clients or any member of their group howsoever obtained. In maintaining confidentiality hereunder the Recipient Party agrees, accepts, warrants and covenants that it shall not, either on its own account or jointly with or for any other person, firm, company or any other entity, without obtaining the written consent of the disclosing party;

1. disclose, transmit, reproduce or make available any such Confidential Information to any person firm, company or any other entity other than its directors, partners, advisers, agents or employees, who need to know the same for the purpose of evaluating, preparing, considering, negotiating, advising in relation to or in furtherance of the purpose aforesaid; or
2. use the Confidential Information for any purpose other than evaluating, preparing, considering, negotiating, advising in relation to or in furtherance of the purpose mentioned aforesaid; or
3. disclose, announce or otherwise publicize the existence of its association with the Disclosing Party or the existence of the project with the Disclosing Party or any other arrangement (existing or possible) between the disclosing party, its clients or itself in connection with any project/assignment; or
4. use any such Confidential Information for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its clients or any member of their group or their projects.
   1. The Recipient Party also agrees, accepts and warrants that it shall:
5. use at least the same degree of care in safeguarding such Confidential Information as it uses for its own Confidential information of like importance and such degree of care shall be at least that which is reasonably calculated to prevent such inadvertent disclosure;
6. keep the Confidential Information and any copies thereof secure and in such a way so as to prevent unauthorised access by any third party;
7. limit access to such Confidential Information to those of its directors, partners, advisers, agents or employees who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees so involved to protect the Confidential Information in the manner prescribed in this Agreement; and
8. upon discovery of any disclosure or suspected disclosure of Confidential Information, to promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Information, in whatsoever form, including any and all copies thereof.

**3. Return or destruction:**

The Recipient Party shall, upon completion of the purpose mentioned aforesaid or at any time on receipt of a written demand from the disclosing party:

1. immediately return all written Confidential Information and all copies thereof provided to, or produced by, it or its advisers, as the case may be, which is in such party’s possession or under its custody and control;
2. to the extent practicable, but without prejudice to the obligations of confidentiality herein, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the other party;
3. so far as it is practicable to do so (but, in any event, without prejudice to the obligations of confidentiality contained in this Agreement), immediately expunge any Confidential Information relating to the Disclosing Party or its clients or any member of their group or their projects from any computer, word processor or other device in its possession or under its custody and control; and
4. to the extent practicable, but without prejudice to the obligations of confidentiality herein, immediately furnish a certificate signed by its director or other responsible officer confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.
5. **Permitted disclosure:**

The provisions of paragraph 2 shall not restrict any disclosure required by law or by order of any court of competent jurisdiction, the rules and regulations of any recognised stock exchange or any enquiry or investigation by any governmental, official or regulatory body which is lawfully entitled to require any such disclosure and if so the Recipient Party shall disclose only to the extent of the Confidential Information required to be disclosed under the Order, rules or statue provided that, so far as it is lawful and practical to do so prior to such disclosure, the Recipient Party shall promptly notify the other party of such requirement with a view to providing the opportunity for the Provider to contest such disclosure or otherwise to agree the timing and content of such disclosure.

1. **No Representation:**

Neither the disclosure, transmission receipt or exchange of Confidential Information nor anything else in this Agreement will constitute an offer by or on behalf of the Disclosing Party or be construed as soliciting any business or organization changes or any assurance of any business commitment or an inducement to incur / undertake any obligations not specified herein and neither party will be under any obligation to accept any offer or proposal which may be made by the other or on behalf of such other party. Neither the Confidential Information nor anything else in this Agreement will commit or bind the other party to enter into a contract or otherwise or form the basis of any contract which will be constituted solely by any final agreement(s) negotiated and entered into between the parties to this Agreement.

1. **No Assignment:**

This Agreement shall not be assigned by either party, by operation of law or otherwise, without the prior written consent of the other party. This Agreement shall inure to the benefit of and will be binding upon the parties’ respective successors and permitted assigns.

1. **Severability:**

In the event that any of the provisions contained in this Agreement is found to be invalid, illegal or unenforceable in any respect by a Court of competent jurisdiction, the validity, legality, or enforceability of the remaining provisions contained in this agreement will not be in any way affected or impaired by such a finding.

1. **Delay or Waiver:**

No delay or failure of either Party in exercising any right hereunder and no partial or single exercise thereof shall be deemed of itself to constitute a waiver or an expectation of non-enforcement of such right or any other rights hereunder. No waiver of any provision of this Agreement shall be valid unless the same is in writing and signed by the party against whom such waiver is sought to be enforced. A waiver or consent given by either party on any one occasion is effective only in that instance and will not be construed as a bar to or waiver of any right on any other occasion.

1. **Notices:**

Notices as required by this Agreement shall be sent to the Parties at the addresses mentioned first herein above or such other addresses as the Parties may designate from time to time, and shall be sent by certified or registered mail with acknowledgement due on receipt.

1. **Dispute Resolution & Governing Law:**

Any dispute or disagreement arising between the Parties in connection with the interpretation of any Article or provision of this Agreement, or the compliance or noncompliance therewith, or the validity or enforceability thereof, or any other dispute related to this Agreement which is not settled to the mutual satisfaction of the Parties within thirty (30) days (or such longer period as may be mutually agreed upon) from the date that either Party informs the other, in writing, that such dispute or disagreement exists, shall be settled by arbitration. Such arbitration shall be held in Bengaluru and be conducted in the English Language and all issues and matters arising therein shall be construed in accordance with and be governed by the provisions of Arbitration and Conciliation Act, 1996 and Rules framed thereunder as may be amended from time to time. The arbitral tribunal shall be comprised of a sole arbitrator to be appointed by mutual consent of the parties failing which the Arbitrator shall be Appointed in accordance with the Arbitration and Conciliation Act,1996. The award of the arbitral Tribunal shall be final and conclusive and binding upon the Parties, The rights and obligations of the Parties under, or pursuant to, this Clause, including the arbitration agreement in this Clause, shall be under the exclusive jurisdiction of the Courts at Bengaluru and shall be in accordance with the Laws of India.

1. **Term**

This Agreement shall commence from the Effective Date of this Agreement and shall be valid for a period of **\_\_\_\_\_\_\_\_\_** years there from. Either Party may terminate this Agreement for breach, if the defaulting Party fails to rectify the breach within one month notice period issued by the non-defaulting Party. Notwithstanding the above, the obligations of the parties under this Agreement shall be in force for two years from the date of expiry or effective date of termination

1. **Entire Agreement:**

This Agreement, including all Annexures, Exhibits and Schedules (if any) attached hereto, shall constitute the entire agreement amongst the parties hereto. It shall supersede all prior or contemporaneous oral or written communications, proposals, conditions, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgement or other communication between the parties relating to its subject matter during the term of this Agreement.

1. **Headings:**

The headings given herein above are for easy reference only and shall not attach or have any effect/ meaning whatsoever contrary to what is stated in the agreement.

1. **Counterparts:**

This Agreement has been signed in duplicate, each of which shall be deemed to be original.

IN WITNESS WHEREOF THE PARTIES HERETO HAVE CAUSED THIS AGREEMENT TO BE EXECUTED BY THEIR AUTHORIZED REPRESENTATIVES ON THIS \_\_\_\_\_\_\_ DAY OF \_\_\_\_\_ 2020.

Signed and delivered by Signed and delivered by

**For \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ For BEML LIMITED**

Signed by: Signed by:

Name: Name:

Title: Title:

Witnesses: Witnesses:

1. 1.
2. 2.