

**CORRIGENDUM FOR TENDER NO: 6300034088 Dated 03.09.2020**

SI No	RFP Page No	Section No / Clause	FOR	READ AS:
1	45 & 81	Technical bid Bidder Criteria details Point No. 7	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. <b>02 Crores</b>  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. <b>XX Crores</b>	Revised Clause "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 <b>Rs. 1.2 Crores</b> "
2	6	III - Clause 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).	Revised Clause "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 based on mutually agreed additional cost between BEML and bidder).
3	7	III - Clause 6	Continually ensure 100% log sources of BEML Systems should integrate with proposed SIEM	Revised Clause "Continually ensure 100% log sources of BEML Systems, as indicated in existing infrastructure (section II), should integrate with proposed SIEM."
4	7	SOC Deliverables - Clause 16	Training for Maximum of 5 and Complete Documentation to be given to BEML identified team	Revised Clause "Training for Maximum of 5 personnel and Complete Documentation to be given to BEML identified team."
5	10	On-Premise Operation Team Specification	Monitoring & Tracking Incidents / Alerts 10x6, Reporting & Escalation, Regular SIEM Administration (L1).	Revised Clause "Monitoring & Tracking Incidents / Alerts 12x6, Reporting & Escalation, Regular SIEM Administration (L1)."
6	11	On-Premise Operation Team Specification	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.	Revised clause: 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. No additional cost will be paid for extended working hours and on Sundays/holidays
7	12	IV - Clause 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.	Revised Clause " The Bidder's proposed SIEM Solution shall be rated in Gartner magic quadrant for Security Information and Event Management in any of the last three years for which this rating is published ( <b>or</b> ) 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 ( <b>or</b> ) Gartner's Magic Quadrant shall be submitted as a part of technical bid."
8	12	IV - Clause 4	The selected Bidder shall supply, install, customize, integrate, migrate, test, and troubleshoot the SIEM to run SOC; subcontracting or consortiums are not allowed.	Revised Clause "The selected Bidder shall supply, install, customize, integrate, migrate, test, and troubleshoot the SIEM to run SOC; consortium is not allowed, Sub-contracting is allowed as per Section - XI of the tender."

**CORRIGENDUM FOR TENDER NO: 6300034088 Dated 03.09.2020**

SI No	RFP Page No	Section No / Clause	FOR	READ AS:
9	25	Anti-phishing Services: Clause 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.	Revised Clause : " 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 BEML in identifying customers affected by phishing attacks." This is services, bidder should implement the available best practices of security in consultation with BEML.
10	27	Training, Clause c)	c) 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.	Revised Clause "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 or OEM certified trainer for a period of 5 days"
11	31	VI. 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).	Revised Clause " This Tender is for 1 year warranty period & 3 year support(AMC) period, further BEML wishes to extend further 2 years OEM & bidder shall support the same. i.e., 1 (W) + 3 (AMC) + 2 (AMC with extension of this contract with pro-rata basis)."
12	45 & 81	Criteria details, Clause 3	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	Revised Clause "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, PKI, SSO, IDAM, DLP, MDM, Anti-DDoS, NAC, and Vulnerability Management in the last 5 years
13	48	Page 48. PART C – Clause 4	4. EDR Management server - 1	Revised Clause "At present as per our specification HA is not required."
14	61	Annexure - D, Clause 4	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.	Revised Clause " The total retention period to be accommodated is 3 months (online)+ 9 months (online) + 4 years (offline). The online storage should be connected with SIEM and data on the same should be available for investigation and reporting at any given point in time without having to restore the same with separate process. Whereas the data that is aged beyond 1 year (3 months (online) + 9 months (online)) shall be purged into offline storage, and the offline storage shall be in the form of Backup media and Built in storage. For the offline data retention the bidder must leverage and provide the existing BEML backup solution / NAS / purpose built backup storage. But the bidder has to recommend the total storage required for 4 year offline retention, so that the tape media shall be arranged by the BEML."

**CORRIGENDUM FOR TENDER NO: 6300034088 Dated 03.09.2020**

SI No	RFP Page No	Section No / Clause	FOR	READ AS:
15	73	Annexure - F, Clause 3,4,5,6	3.A full packet capture software should be provided with 256 Mbps line rate with multiple ingress interfaces for capturing from multiple network interfaces. 4.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. 5.The Solution should have endpoint threat detection agent supporting all major operating systems like Windows etc., 6.There should be a single dashboard with integrated and native correlation between logs and EDR solution	Revised Clause " These requiremnets are Mandatory Requirements. All these points are moved to Annexure - D under Section B." 4. The solution Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including image views, artefact & raw packet and object extractions. Bidder should have supplied the proposed packet capture solution to atleast one customer in India.
16	73	Annexure - F, Section B, Clause 1	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.	Revised Clause "The proposed SIEM solution should have built-in STIX/TAXI support to integrate with open source Threat Intelligence Platform (TIP) integration capability. The proposed SIEM solution tool should also have REST API support to integrate with any 3rd party SOAR platform that BEML may procure in the future"
17	68	Annexure - F, Clause 33	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.	Revised Clause " The solution should support way to define alert criticality and leverage the same in Incident risk score, the must be adjustable for better priorisation during incident management"
18	71	Annexure - F, Clause 59	Reports should be available in pdf, csv, word and html format.	Revised Clause "Reports should be available in pdf, and optionally in csv, word and html format."
19	72	Annexure - F, Clause 66	The solution must support the ability to centrally deliver asset reports.	Revised Clause " The solution should be able import Asset Management data for event data enrichment"
20	72	Annexure - F, Clause 75	End user & Admin access with required licenses should be included for unlimited users.	Revised Clause" The solution must accommodate at maximum number of 10 admin user license access to the SIEM console"
21	6		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)	Revised Clause : " All SOC activities to be automated would be a challenge with only SIEM solution. Case management would be manual. Management of individual solution eg. EDR, Packet Capture would be manual."
22	6 & 33		Required Uptime 97% and above . Penalty - NA	Revised Clause : " The SOC infrastructure must support all features, functionalities etc. on real time and with 97.00% uptime on quarterly basis at each layer of solution for enterprise-wide infrastructure of the BEML including those operational at Data Centers."
23	12	IV - Clause 3	Proof of compliance to the above referred notification & Gartner's Magic Quadrant shall be submitted as a part of technical bid.	Revised Clause " Proof of compliance to the above referred notification <b>(or)</b> Gartner's Magic Quadrant shall be submitted as a part of technical bid."
24	22	V.Services	a)The Bidder shall carry out PT for all public IPs (not exceeding 25) of BEML on a half yearly basis.	Revised Clause " a)The Bidder shall carry o external t PT for all public IPs (not exceeding 25) of BEML on a half yearly basis."

**CORRIGENDUM FOR TENDER NO: 6300034088 Dated 03.09.2020**

SI No	RFP Page No	Section No / Clause	FOR	READ AS:
25	44	Clause 3	3.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	Revised Clause "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, PKI, SSO, IDAM,DLP, MDM, Anti-DDoS, NAC, and Vulnerability Management in the last 5 years
26	68	Annexure - F	35 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.	Revised Clause : The solution must provide mechanism to consume asset classification data to enrich the event log collected by SIEM and better prioritize the alerts/incidents
27	72	Annexure - F	89. System should support online asset classification by asset owners, based on rating attributes (not limited to) - Criticality rating - Confidentiality rating - Integrity rating - Availability rating	Revised Clause :The system should support event log enrichment with asset classification by asset owners, based on rating attributes (but not limited to) - Geo location - Event Severity or Criticality rating - Event Group - Event name, Event Severity Category, Sequence Number and Event Type and the Device and Application associated with the Events
28	69	Annexure - F	39. "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"	Revised Clause " The solution should support way to define alert criticality and leverage the same in Incident risk score, the must be adjustable for better prioritization during incident management"
29	71	Annexure - F	75. End user & Admin access with required licenses should be included for unlimited users.	Revised Clause" The solution must accommodate at min of 5 user license access to the SIEM console"

**CORRIGENDUM FOR TENDER NO: 6300034088 Dated 03.09.2020**

SI No	RFP Page No	Section No / Clause	FOR	READ AS:
30		Annexure F Page no. 65	<p>1 Minimum specification of each layer to be as below:</p> <p>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</p> <p>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</p> <p>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.</p> <p>EDR Management server:- Qty 1 No. 4 Core, 16GB RAM, 500 GB HDD Windows 2019, MS SQL 2016 SP1</p>	<p><b>Revised Clause to Annexure F Point 1.</b></p> <p>1 Minimum specification of each layer to be as below: Log Collection: - Qty 2 Nos. - 2 No in DC, 1 No in DR 16-core Intel Xeon, 2.1 GHz CPU 64 GB RAM 4 TB HDD (usable) RAID5 (HA Not required)</p> <p>Log Management: - Qty 1 No. - 1 No in DC 24-core Intel Xeon, 2.3 GHz CPU 192 GB RAM 24 TB HDD (usable) RAID5</p> <p><b>Packet Capture Management: - Qty 1 No. - 1 No in DC, 24-core Intel Xeon, 2.3 GHz CPU 192 GB RAM 24 TB HDD (usable) RAID5</b></p> <p>Log Correlation: - Qty 1 No. - 1 No in DC, 32-core Intel Xeon, 2.1 GHz CPU 256 GB RAM 5 TB HDD (usable) - RAID10.</p> <p>EDR Management server:- Qty 1 No. - 1 No in DC. 4 Core, 16GB RAM, 500 GB HDD Windows 2019, MS SQL 2016 SP1</p> <p>Storage for Archive: - Qty 1 No. - 1 No in DC. 55 TB – 10k RPM SATA/SAS/FC Bidder Need to propose the SIEM OEM appliance with required specifications so has to handle as per Annexure - D Point No 2. Bidder shall size accordingly where as SIEM OEM shall confirm in writing that the specification will meet the requirements as per EPS mentioned in point no. 2 Annexure - D as per industry best practices. The same should be mentioned in Technical Bid. If bidder is proposing software based SIEM solution, the required server and storage hardware must be proposed from the reputed OEMs like IBM/Dell/Cisco/HPE/EMC etc.,</p> <p>The hardware configuration provided is minimum requirement and bidder need to propose the required hardware configurations as per the recommendation from SIEM OEM.</p> <p>Bidder need to provision required minimum physical/virtual infrastructure for running the proposed SOC solution.</p>
31				

**CORRIGENDUM FOR TENDER NO: 6300034088 Dated 03.09.2020**

SI No	RFP Page No	Section No / Clause	FOR	READ AS:
32		IV. PRODUCTS Page no. 13 Security Information and Event Management	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.	Revised Clause : The SOC team should configure the policies in the SIEM for automating the backup from SIEM to the purpose built backup storage for archival retention policies.
33		IV. PRODUCTS Page no. 15 Security Information and Event Management	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.	Revised Clause :.Both Online & offline logs should be stored in built-in storage. Only for archival logs purpose built backup storage shall be considered as per the 4 Year retention policy i.e., minimum 55 TB to be considered.
34	6		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	Revised Clause : The SOC infrastructure must support all features, functionalities etc. on real time and with 97.00% uptime on quarterly basis at each layer of solution for enterprise-wide infrastructure of the BEML including those operational at Data Centers
35	19		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	Revised Clause : The proposed 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
36	21		The expert should be available at the site of the incident within 12 hrs.	Revised Clause : ii. The expert should be available at the site of the incident within 48 hrs.
37	18		1. 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.	Revised Clause : 1. Bidder shall monitor all 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.
38	14	IV.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.	Revised Clause "All the components of proposed SIEM solution at BEML including SIEM appliance/software, log collection devices, storage system should have hot-swappable dual power supply." Bidder who are proposing software based SIEM solution, the required server and storage hardware must be proposed from the reputed OEMs like IBM/Dell/Cisco/HPE/EMC etc.,  The hardware configuration provided is minimum requirement and bidder need to propose the required hardware configurations as per the recommendation from SIEM OEM.
39	61	Annexure D.1	The proposed appliance should be SIEM OEM appliance. The SIEM OEM should have end to end support for this appliance.	Revised Clause "The proposed appliance should be SIEM OEM appliance. The SIEM OEM should have end to end support for this appliance/software." Bidder who are proposing software based SIEM solution, the required server and storage hardware must be proposed from the reputed OEMs like IBM/Dell/Cisco/HPE/EMC etc.,  The hardware configuration provided is minimum requirement and bidder need to propose the required hardware configurations as per the recommendation from SIEM OEM.

**CORRIGENDUM FOR TENDER NO: 6300034088 Dated 03.09.2020**

SI No	RFP Page No	Section No / Clause	FOR	READ AS:
40	67	Annexure - F . A.18	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.	Revised Clause : Next gen SOC solutions shall forward logs to log management layers deployed at same site and can auto replicate logs. This shall avoid log loss and avoid duplication of logs. Bidder to make sure that same logs are available at both sites.
41	67	Annexure - F . A.25	Every log event should be given a unique event id so that event can be tracked across multiple layers of SIEM.	Revised Clause : Bidder shall need provide a next generation solution which can do Risk based alerting which can reduce the number of false positives from alerts and bring up only critical high risk alerts or incidents.
42	70	Annexure - F . A.46	Normalization of events collected should be performed on all events received by the system proposed so as to ensure that all logs are queryable and drillable. Also, normalization should happen at collection layer or collectors.	Revised clause : Solution should be able to query on raw logs and run correlation and analytics on raw logs.
43	71	Annexure - F . A.72	Proposed SIEM solution should have data science engine which enables analysts to do predictive analysis in reports.	Revised clause : SIEM solution should have OOTB of the machine learning models to Predict Numeric Fields, Categorical Fields, Detect Numeric Outliers, Detect Categorical Outliers, Forecast Time Series etc.  SIEM solution should have development tool to enable users to create, validate, manage, and operationalize machine learning models through a guided user interface.
44			The solution must provide alerting based upon established policy. (e.g., IM traffic is not allowed.)	Revised Clause : "The solution must provide alerting based upon established policy / rules. (e.g., logs for IM traffic is not allowed.). "
45			The solution should allow creating custom log source lists to provide a direct mapping for log sources that fall in-scope for regulatory compliance	Revised Clause "The solution should allow creating custom log sources and eventtypes and should provide a direct mapping for log sources to the regulatory compliance group. "
46			Proposed SIEM solution should have data science engine which enables analysts to do predictive analysis in reports.	Revised Clause "Proposed SIEM solution should have the option to define value which enables analysts to do predictive analysis for performance. Network utilization, file access based on the base line value or defined performance, network utilization bandwidth values "
47			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).	Revised Clause : " The distributed can be the collectors or the rule engine processing components like Worker "

**CORRIGENDUM FOR TENDER NO: 6300034088 Dated 03.09.2020**

SI No	RFP Page No	Section No / Clause	FOR	READ AS:
48			<p>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</p> <p>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</p>	<p>Revised Clause "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, PKI, SSO, IDAM, DLP, MDM, Anti-DDoS, NAC, and Vulnerability Management in the last 5 years</p> <p>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</p>
49	Page 6	,III SCOPE OF WORK & TECHNICAL SPECIFICATIONS	<p>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 <b>future gateway security appliances</b> with no/minimum possible downtime.</p>	<p>Revised Clause : 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 <b>future gateway security appliances will be based on open standards and support SIEM integration</b> with no/minimum possible downtime.</p>
50	Page 27	Continuous Improvement	<p>e) Bidder has to integrate with proposed SOC at least 12 additional security devices/tools during the lifecycle of the project.</p>	<p>Revised Clause : Bidder has to integrate with proposed SOC at least 12 additional security devices/tools during the lifecycle of the project <b>based on open standards and support integration with industry standard SIEM.</b></p>
51	Page 27	Training	<p>J) 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</p>	<p>Revised Clause : The bidder / 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 ( <b>8 Hrs</b> ). BEML has the right to exercise this training option at its discretion</p>