Online Request for Proposal (e-RFP)

For

Endpoint Detection & Response (EDR) Solution with Advanced XDR Capabilities

e-RFP Ref. No.JKB/CHQ/ISD/EDR-Sol/2026-1714
Dated: 29-04-2026

SCHEDULE OF RFP

1. Bid Schedule

e-RFP Reference No.	JKB/CHQ/ISD/EDR-Sol/2026-1714 Dated: 29-04-2026
Date of Issue of RFP	30-04-2026
RFP Description	Endpoint Detection & Response (EDR) Solution with Advanced XDR Capabilities
Issuer of the RFP-Department	Information Security Department, Corporate Headquarters, M.A. Road Srinagar 190001 J&K
Bank's Communication Details	J&K Bank Information Security Department, Corporate Headquarters, M.A. Road, Srinagar 190 001 LL. No.: 0194-2713254/0194-2713386 Mobile No: e-mail: info.security@jkbmail.com
RFP Application Fee (Non - Refundable)	Rs.5000/- (Rupees Five Thousand Only) to be deposited through Transfer / NEFT only to below a/c : Account Name: Tender Fee/ Cost Account 16-digit Account No : 9931530300000001 IFSC Code: JAKA0HRDCHQ (0 denotes zero) Bank: The J&K Bank Ltd Branch: Corporate Headquarters MA Road Srinagar J&K - 190001 UTR Number / Tran No. & Date may be uploaded as proof on

Earnest Money Deposit (EMD) (Refundable)	₹ 24,00,000/- (Rupees Twenty Four Lacs Only) to be deposited through Transfer / NEFT only to below A/c: Account Name: Earnest Money Deposit (EMD) 16-digit Account No : 9931070690000001 IFSC Code: JAKA0HRDCHQ (0 denotes zero) Bank: The J&K Bank Ltd Branch: Corporate Headquarters MA Road Srinagar J&K - 190001 UTR Number & Date / Tran No. & Date may be uploaded on e-Tendering Portal as Proof of the EMD (EMD is exempted for all Start-ups as recognized by DPIIT/DIPP)
Bid Document Availability including changes/amendments, if any to be issued	NIT can be downloaded from and submitted on Bank's e-Tendering Services Provider's Portal https://jkbank.abcprocure.com from April 30, 2026 16.00 Hrs. to May 21, 2026 17.00 Hrs.
Last Date for Pre-Bid Queries & submission Mode	All Clarifications / Queries shall be raised online only through e-Tendering Portal https://jkbank.abcprocure.com by or before April 07, 2026 17.00 Hrs.
Pre-bid Queries Response date	All communications regarding points / queries requiring clarifications shall be given online through prescribed e-Tendering Portal on April 13, 2026
Last Date of Submission of RFQ Bid	May 21, 2026 17.00 Hrs.
Submission of online Bids	As prescribed in Bank's online tender portal https://jkbank.abcprocure.com
Date and time of opening of technical bid	To be notified separately

<table>
<tr><td>Corrigendum</td><td>All the Corrigendum will be uploaded on online tender portal https://jkbank.abcprocure.com only</td></tr>
<tr><td>For e-Tender related Queries</td><td>Service Provider:
M/s. E-procurement Technologies Limited
(Auction Tiger) , B-705, Wall Street- II, Opp. Orient Club, Ellis Bridge, Near Gujarat College,
Ahmedabad- 380006, Gujarat
Help Desk:
<table>
<tr><th>Sr. No</th><th>Name</th></tr>
<tr><td>1</td><td>Sandhya Vekariya - 6352631968</td></tr>
<tr><td>2</td><td>Suraj Gupta - 6352632310</td></tr>
<tr><td>3</td><td>Ijlalaehmad Pathan - 6352631902</td></tr>
<tr><td>4</td><td>Imran Sodagar - 9328931942</td></tr>
</table></td></tr>
</table>

DISCLAIMER

The information contained in this RFP document, or any information provided subsequently to bidder(s) whether verbally or in documentary form/email by or on behalf of the J&K Bank is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP is neither an agreement nor an offer and is only an invitation by the J&K Bank to the interested parties for submission of bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. While effort has been made to include all information and requirements of the Bank with respect to the solution requested, this RFP does not claim to include all the information each bidder may require. Each bidder should conduct its own investigation and analysis and should check the accuracy, reliability and completeness of the information in this RFP and wherever necessary obtain independent advices/clarifications. The Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. The Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. The Bank and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on it.

The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP. Failure to furnish all information required under this RFP or to submit a Bid not substantially responsive to this RFP in all respect will be at the Bidder's risk and may result in rejection of the Bid.

The issue of this RFP does not imply that the Bank is bound to select a Bidder or to award the contract to the Selected Bidder, as the case may be, for the Project and the Bank reserves the right to reject all or any of the Bids or Bidders without assigning any reason whatsoever before issuance of purchase order and/or its acceptance thereof by the successful Bidder as defined in Award Criteria and Award of Contract in this RFP.

The Bidder shall, by responding to the Bank with a bid/proposal, be deemed to have accepted the terms of this document in totality without any condition whatsoever and accepts the selection and evaluation process mentioned in this RFP document. The Bidder ceases to have any option to object against any of these processes at any stage subsequent to submission of its responses to this RFP. All costs and expenses incurred by interested bidders in any way associated with the development, preparation, and submission of responses, including but not limited to the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by J&K BANK, will be borne entirely and exclusively by the Bidder.

The bidder shall not assign or outsource the works undertaken by them under this RFP assignment awarded by the Bank without the written consent of the Bank. The Bidders can take advantage of any Government order which applies to any tendering process and whereby there is any relaxation that is in conflict with the terms and conditions mentioned in this RFP, if and only if, any such Government order/ notification comes into force before the last date of submission of bids. Further, in case of any such orders that may affect/ contradict with the terms and conditions of this RFP, the Bidders need to seek clarification through the online procurement portal before the last date for submission of bids. The Bidder hereby agrees and undertakes to Indemnify the Bank and keep it indemnified against any losses, damages suffered and claims, action/ suits brought against the Bank on account of any act or omission on part of the Bidder, its agent, representative, employees and sub-contractors in relation to the performance or otherwise of the Services to be provided under the RFP. The bidders shall not assign or outsource the works undertaken by them under this RFP awarded by the Bank, without the written consent of the Bank.

CONTENTS

A. INTRODUCTION

Brief About Bank:

The Jammu and Kashmir Bank Limited (J&K Bank / Bank) having its Corporate Headquarters at M.A Road Srinagar, J&K -19001 has its presence throughout the country with 1000+ Branches and more than 1400 ATMs. The Bank uses Information Technology in all spheres of its functioning by connecting all its branches and offices through its WAN.J&K Bank functions as a universal Bank in Jammu & Kashmir and as a specialized Bank in the rest of the country. Bank functions as a leading bank in the Union Territories of Jammu & Kashmir and Ladakh and is designated by Reserve Bank of India as its exclusive agent for carrying out banking business for the Government of Jammu & Kashmir and Ladakh. J&K bank caters to banking requirements of various customer segments which includes Business enterprises, employees of government, semi-government and autonomous bodies, farmers, artisans, public sector organizations and corporate clients. The bank also offers a wide range of retail credit products, including home, personal loans, education loan, agriculture, trade credit and consumer lending, a number of unique financial products tailored to the needs of various customer segments. The Bank, incorporated in 1938, is listed on the NSE and the BSE. Further details of Bank including profile, products and services are available on Bank's website at **https://jkb.bank.in/**.

Purpose of RFP

The purpose of the RFP is to seek proposals from prospect bidders for Supply of Enterprise wide EDR Solution with XDR Readiness Capabilities including its implementation and 3 years support Services. The solution has to be comprehensive, adaptive, and unified cybersecurity protection suite that goes beyond traditional endpoint protection. It must ensure real-time detection, investigation, and response to threats while extending visibility across the entire IT ecosystem.

Jammu & Kashmir Bank Ltd. (J&K Bank) seeks to procure, implement, and maintain a comprehensive Extended Detection and Response (XDR) solution to strengthen cybersecurity across its enterprise.

The solution must have following capabilities into a centralized management platform:

- Endpoint Protection (EPP)
- Endpoint Detection & Response (EDR)
- Application Control (ACC) for blacklisting & whitelisting of applications

The contract will be valid for 3 years. The scope of work is described in detail in – "Scope of Work" of this RFP document. Bank seeks comprehensive quotes from "bidders" who have the capabilities to meet Bank's requirements and have a serious interest in providing the licenses. This RFP provides information on Bank and the requested scope of work, and instructions for the preparation and submission of the RFP Response by the bidder to perform the scope of work.

Bidders who are interested in participating in the RFP must fulfil the eligibility criteria mentioned in the document. Bidder must agree to all our terms & conditions mentioned under this RFP.

Objectives

The XDR solution shall:

- Deploy a centralized, AI-driven platform for holistic endpoint and workload security.
- Detect, analyse, and respond to cyber threats in near real-time.
- Enable automated threat correlation, root-cause analysis, and proactive threat hunting.
- Integrate seamlessly with the Bank's SOC/SIEM (IBM QRadar) and other security tools.
- Ensure compliance with:
    - RBI Master Direction on IT Governance, Risk, Controls, and Assurance (2023)
    - CERT-In guidelines
    - Industry standards and best practices: NIST, ISO 27001, MITRE ATT&CK
    - Proposed solution and its associated services like management, sandboxing etc. must reside On-Premises with access limited to India judiciary boundary with unique URL to dedicated tenant.

Eligibility Criteria

J&K Bank shall scrutinize the Eligibility bid submitted by the bidder. A thorough examination of supporting documents to meet each eligibility criteria (Annexure D) shall be conducted to determine the Eligible bidders. Bidders not complying with the eligibility criteria are liable to be rejected and shall not be considered for Technical Evaluation.

The bidders meeting the General Eligibility Criteria as per Annexure D will be considered for technical evaluation. Any credential/supporting detail mentioned in "Annexure D – Compliance to Eligibility Criteria" and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a Bidder can provide.

Scope of Work

The Bidder shall be responsible for supply, installation, implementation and management of the following modules as a part of the Centralized Endpoint and Server Protection Solution:

1. Enterprise Antivirus Solution/Endpoint Protection (EPP) with the following features
    a. Anti-Virus
    b. Anti-Malware
    c. Antispyware,
    d. File Reputation
    e. Exploit Prevention (host firewall, exploit protection)
    f. Command and Control (C&C) protection
    g. Zero-day Vulnerability Protection
    h. Device Control
    i. Ransomware Protection
    j. Desktop Firewall & Host Intrusion Prevention
    k. Browser IPS
    l. Application Control or File discovery
    m. Machine Learning-driven Exploit
    n. Network Integrity, Wi-Fi Reputation, and Smart VPN
    o. Active Directory Defence
    p. Active Directory Breach Assessment
    q. Adaptive Security
    r. Threat Intelligence API

s. Isolation
t. Mobile Threat Protection/Defence
u. File Integrity Monitoring

2. Endpoint Detection & Response (EDR) and Extended Detection & Response (XDR)
3. Endpoint Encryption
4. Server Security
5. Setup and Implementation of the complete solution at DC and DR including Integration with various endpoints and security solutions.
6. The bidder should take care of Supply, Implementation, Maintenance and support of end point security solutions at all the endpoints and machines at all Bank's locations including branches, Cluster Offices, Zonal Offices etc. and which are connected to Bank's Data Center and DR through MPLS, Leased line, RF/VSAT, 4G/5G etc.
7. All the jobs / tasks / Blockade / application blacklist / whitelist etc. on present Application is to be incorporated along with necessary reports (success / failure of jobs etc.) on proposed Application.

Supply of Solution

1. The Bidder is required to design, size supply, implement & maintain the solution at Bank's DC and DR locations during the tenure of the contract. The supplied solution must be able to protect Bank's infrastructures such as Desktops, Laptops, Tablets, Servers, etc. at all the locations including Bank Branches, Circle offices and Zonal offices and other JK Bank's office locations.
2. The Bidder shall quote for the solution, which should be able to cater to more than 13 thousand endpoints for Bank. All the technical specifications and features as mentioned in the RFP must be deployed by the bidder. The solution should be further scalable to the adequate capacity as per the business requirements of the Bank.
3. The minimum server specifications for the solution to be proposed by the Bidder.
4. Below is the tentative requirement of the Bank. The initial tentative estimated requirement is of approx. 11500 licenses. In case of future requirement Bank shall place the additional order at same rates, terms and conditions.
5. The solution should take care of updating of antivirus on devices/endpoints in offices connected through MPLS VPN, Leased line, RF/VSAT, 4G/5G along with Servers at DC & DR Site.

6. The public Cloud based solutions should not be proposed under this RFP and if proposed, shall not be considered. Bidder should propose on-premises solution only for complete solution as per RFP.
7. The solution has to be installed each at DC (at present in Noida) and at DR (at present in Mumbai) in HA at each site. In addition, the solution should be capable to work in active-active mode between DC & DR with an option to shift/bifurcate the load at each location. The solution setup at DR should be an exact replica of the solution setup at DC i.e., configuration, security policy etc. must be in sync at each site DC & DR and if either fails, the other setup should be able to handle/cater the complete load. The bidder should ensure that there is no single point of failure in the solution at any point of time. In case Bank shifts it's DC and/or DR to any other location during the tenure of the contract, vendor shall be responsible for de-installation, re-installation and migration (if required) of the entire solution without any additional cost to the Bank. Transportation and insurance during such shifting activity shall be the responsibility of the Bank.
8. The bidder should setup the endpoint security solution for JK Bank in HA at each site (DC and DR) to ensure that JK Banks endpoints/devices are addressed as per RFP requirement.
9. All terms & conditions and Scope of work applicable for DC shall be applicable for DR as well. Any software required to synchronize DC setup & DR setup of this solution should be provided by the bidder.
10. The Bidder shall provide details of each hardware and software component such as number of licenses factored, make and model, specifications, license type, etc. and their price breakup of each component in the Commercial Price Bid on a separate sheet
11. No freeware or unlicensed/unsupported open-source software should be proposed as part of the solution and Bidder shall have to ensure the same.
12. The responsibility of Bidder shall be to maintain, manage and support including patches, updates and upgrades implementation of EPP, EDR & XDR across all JK Banks offices and branches.
    a. The Bidder must provide a mechanism to ensure regular updates of Antivirus Updates, patches, virus definitions on desktops and servers.
    b. The bidder should propose a solution, which should be flexible in deployment. Solution should be supported on-premises, cloud managed, and hybrid models.

c. A single unified agent is mandatory for Anti-Virus, Anti-Malware, Antispyware, File Reputation, Exploit Prevention, Command and Control (C&C) protection, Zero-day Vulnerability Protection, Device Control, Ransomware Protection, Desktop Firewall & Host Intrusion Prevention, Browser IPS, Application Control or File discovery, Active Directory Defence, Active Directory Breach Assessment, Adaptive Security, Threat Intelligence API, Isolation.

13. For all hardware/Appliances and software components, the bidder must provide 3 years warranty from the date of Go-Live of the solution at no extra cost to Bank.
14. The bidder shall ensure to quote 3 years subscription-based licenses for the complete solution as per RFP, and the period/tenure shall be start from the date of implementation.
15. Bidder should ensure that the quoted solution must be as per the scope and technical Specifications given in the RFP. Bidder should implement the solution at all the endpoints (i.e., at Zonal Offices, Cluster Offices, Branches and offices etc.) centrally from DC/DR location. Wherever installation is not feasible centrally, the bidder has to ensure the implementation of endpoint security at particular location manually/physically.
16. The proposed solutions shall be tightly integrated with all existing setup and new infrastructure /Assets of the Bank.
17. The solutions should be designed in such a way that they cover all the divisions of the Bank's Data Centre having separate networks & all separate network segments of each.
18. The proposed solution should be configured and scalable to cater the requirement of the Bank and the solution deployment should be compliant with Bank's IS, IT and Cyber policies, internal guidelines, regulatory requirements and country wide regulations and laws from time to time.
19. In case more than one device/appliance is provided to cater to the above requirements, then it should have the capability to sync all configuration between all devices in case changes are being made on one device from a single management console. In case the syncing requires any external device, the same has to be provided without any additional cost to the Bank.
20. The solution should effectively and efficiently manage operations and security posture of the Bank by preparing for and responding to cyber risks/threats, facilitate business continuity and recovery from cyber-attacks / incidents.

21. Any future upgrades and updates of software should be given free of cost and the solution should support any such upgrade during the contract period without affecting the performance of the solution.
22. The solution should be in adherence to the guidelines provided in the RBI cyber security circular no RBI/2015-16/418 dated 2nd June 2016 and its amendments (in present and in future) and guidelines, advisories. circulars from RBI and any statutory or regulatory body or Govt. of India from time to time. The bidder shall ensure all features and fine-tuning in the solution as per prevailing and future guidelines from RBI, GOI, other regulatory bodies and compliance on advisories from National Critical Information Infrastructure Protection Centre (NCIIPC), CERT-IN, CSITE and other statutory/Govt. bodies.
23. The bidder shall submit deployment methodology as part of project plan inline to the functional requirements of the solution.
24. The bidder should propose solution that identifies rogue Wi-Fi networks, utilizes hotspot reputation technology, and delivers a policy-driven VPN to protect network connections and support compliance.
25. The bidder should include features of EPP that blocks known network and browser-based malware attacks using rules and policies and prevents command and control setup with automated domain IP address blacklisting.
26. The solution should continuously probe Active Directory for domain misconfigurations, vulnerabilities, and persistence using attack simulations to identify risks and allow for immediate mitigation and remediation recommendations.
27. The solution should highlight anomalous sources of suspicious behaviour and reduce overall incident volume, enabling the SOC to focus on activity with the most potential for negative impact.
28. The solution should defend the primary attack surface for lateral movement and domain admin credential theft by controlling the attacker's perception of an organization's Active Directory resources from the endpoint using unlimited obfuscation (meaning fake asset and credential creation).
29. The solution should provide the ability to record and analyze endpoint behaviour to identify Advanced Attack Techniques that may be using legitimate applications for malicious purposes. This data should be enriched with the MITRE ATT&CK framework to help guide incidents responders during investigations.

30. The solution should hunt for high-fidelity incidents and combines the power of advanced machine learning and expert SOC analysts to discover the tools, tactics, and procedures used by adversaries. It should ensure that critical attacks are quickly identified with the relevant context. In addition, it should deliver intuitive access to global security data to augment Bank's threat-hunting efforts.
31. The solution should provide recommendations for automatic policy tuning, adaptations and tasks to improve the security posture. The solution should be implemented centrally at all the endpoints with all the features and components mentioned in the RFP. Partial implementation shall not be accepted. Bank shall review the endpoint security implementation at any point of time before sign-off.
32. The solution should support autonomous security management that learns from admins, the organization, or the community to continuously assess and strengthen the security posture. It should also use Artificial intelligence (AI) guided management for establishing strong security policies with fewer misconfigurations and help improve overall security hygiene and posture.
33. The server security solution should support the most widely used server OS platforms which includes Microsoft Windows and non-Windows platform like Linux (Red Hat, Ubuntu, and Oracle), Solaris & AIX, etc.
34. The Server security solution shall have provision to provide protection against the vulnerabilities exploited by the threat actors.
35. All the patches, versions, upgrades, updates should be applied as and when released by the OEM throughout the contract period without any additional cost to the Bank.
36. Vendors should provide support during the entire period of the contract. In case there is a need to depute additional onsite engineers during any Issue, upgradation, updation process then the vendor has to ensure the same without any additional cost to the Bank. Further, online, telephonic, remote in addition to onsite support should be given for resolving operational issues.
37. The solution should be configured in High Availability (HA) at DC and DR along with Load Balancing functionality to cater the load equally or distribute the traffic on each system equally, if required bidder should factor any other software/hardware to perform the functionality with the solution without any additional cost to bank.
38. The bidder has to ensure that during the contract period, the solution utilization and server's CPU utilization should not exceed 70% and server's RAM utilization should not

exceed 80%. In case the performance is adversely affected or the utilization of any server or any peripheral exceeds the mentioned threshold as above, more than 3 times in a quarter, the vendor is required to upgrade the hardware or solution (as applicable), within one month without any additional cost to the Bank.

39. The Vendor should maintain Uptime of 99.95% monthly for the Solution during the contract period.
40. The solutions should be able to integrate various log types and logging options into SIEM and syslog. The solution should also have inherited feature for logging and alerts.
41. Integrate all the solutions with SIEM to generate alerts for any violations and provide a correlated view of threats and vulnerabilities associated with them along with remediation mechanism.
42. Scope of work applicable for DC will be applicable for DR as well. Any software required to sync DC setup & DR setup of EPP, EDR/ATP, XDR & Server Security solution should be provided by the bidder. The policy replication should be support over WAN also.
43. The EPP, EDR, XDR & Server Security solution should take care of bandwidth while updating of solutions on Desktops in branches connected through MPLS, VPN, Leased line, RF/VSAT, 4G/5G or any other technology Link along with Servers at DC & DR Sites.
44. Bidder should set up proper DC-DR replica configuration for Live Update on both Primary and Secondary Network link.
45. The responsibility of Bidder is to maintain/ manage/ support includes patches, updates and upgrades implementation of EPP, EDR, XDR & Server Security solution across all JK Bank branches, Cluster Office, Zonal Office at DC & DR Site.
46. JK Bank offices the Bidder must provide a mechanism to ensure regular updates of Antivirus Updates, patches, virus definitions on desktops and servers.
47. The Bidder has to ensure that the proposed EPP, EDR should be able to install its agents and send updates / patches and receive status on the available bandwidth during office hours without affecting the normal work of the office.
48. The monthly reports giving information like updated on endpoint / client, non-updated on endpoint clients, version details and any other reports specified by JK Bank should be provided to Head Office, Circle & Zonal, other Offices and branches.
49. In case any problem (bulk issues) occurs in any of the authorized software/application of JK Banks due to proposed solution, Bidder has to coordinate with JK Banks/ Application Vendor / AMC Vendor of JK Bank & resolve the same during the tenure of

contract. In case such issue is attributed to the OEM/OSD of the solution, Bidder shall liaison with the OEM/OSD on priority and ensure deployment of corrective measures through deployment of patches, upgrades, additional hardware as required without any additional cost to the Bank.

50. EPP, EDR, XDR Installation in the endpoint (Desktops/ Laptop), if any issue arises, the bidder's resource shall be responsible to coordinate with AMC partner and ensure resolution of all such issues. However, field support will be done by respective AMC vendors.
51. Bidder shall also submit procedural documents related to SOP, day to day operations, backup, periodic restoration, etc.
52. Bidder shall provide draft implementation plan of EPP, EDR, XDR & Server Security solution along with technical bid. The Bidder will also have to document the post install configuration and settings in a post install system configuration document.
53. Successful Bidder shall submit the detailed implementation strategy/ plan of EPP, EDR, XDR & Server Security solution vetted by respective OEM before implementation.
54. The proposed EPP, EDR, XDR & Server Security solution should be capable to sensitize Endpoints/ Servers etc. for not updated with latest updates and should have capability to allow/ not allow machines to connect into network unless latest updates are done in machine based on group policy of proposed solution.
55. The proposed solution should be capable of integrating with Desktop management solution and patch management solution, wherever applicable.
56. Bidder is also, required to supply, Install/Implement, Configure and Maintain the solution for the period of contract.
57. Bidder is required to provide ATS / AMC / subscription to maintain the same for the period of contract for the components part of this RFP.
58. Bidder should have back-to-back OEM and OSD support services for EPP, EDR, XDR & Server Security solution and all the associated hardware and software components.
59. The Bidder shall be responsible for management of this project and provide timely update to Bank.
60. The migration should be seamless with no or minimal disruption (if required). In case of any downtime required, the same may be made available to the Bidder only after prior approval from the Bank and after-business hours.

61. During the warranty (and Subscription Period) period and ATS, AMC, Subscription period, the bidder is bound to do all software and firmware upgrades, updates of proposed solution to next or required version without extra cost to the Bank, covering all parts and labour from the date of acceptance of the systems by the Bank at the respective location i.e., on-site comprehensive warranty.
62. The bidder shall provide the solutions with complete features (over and above to technical specifications) without any extra cost to the Bank and all functionalities should be available for the Bank.
63. The bidder shall provide complete services for the applications under the scope including installation, implementation, integration, migration, management, maintenance, support (Update & Upgrade of Software and Hardware Firmware), audit compliance and knowledge transfer.
64. The bidder shall be responsible to migrate the existing technologies, if required, with new Proposed solution as per the technical specification along with all features.
65. The Bidder is required to design & size the EPP, EDR, XDR at DC and DR. Currently, Bank has about 11500 endpoints. Keeping in view the future growth, it is envisaged that the endpoints may increase to 20,000 at JK Bank during the tenure of 3 years.
66. The solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network.
67. The solution should include all components and subcomponents like software licenses, accessories, and the bidder should supply other components (if not specified) at no extra cost to the Bank that is required for commissioning of the solution as a part of RFP.
68. The bidder shall follow all respective technical/statutory guidelines, validations should be implemented, checked & verified, and related reports including SOP, Software Integrity Certificate and VAPT Clearance must be submitted, duly certified by OEM to the Bank for sign off the successful installation.
69. Post installation of Solution with its components including OS, VA & PT (Vulnerability Assessment & Penetration Testing) shall be conducted, and Bank InfoSec Team will provide a report to the Successful Bidder. All findings/issues pointed out in the report to be complied/fixed before commissioning and sign-off of the software (All components i.e., Database, application). The InfoSec Team and Other statutory authorities conduct review/ audit of the solutions time to time. All such Audit reports including VAPT Reports to be complied / attended by bidder/OEM within the timelines, during the

entire period of contract also conduct periodic review audit of the database and application.

70. The solution deployment should be compliant with Bank's ISMS, IT and Cyber policies, internal guidelines, regulatory standards and countrywide regulations and laws from time to time.
71. The proposed EPP, EDR, XDR & Server Security solution should integrate with Bank's platforms like Security Operation Centre (SOC), Privileged Identity Management (PIM), and Security Incident Event Management (SIEM) (including SOAR or any other security solution implemented in Bank) to meet security and compliance requirements as and when required.
72. The bidder must submit detailed architecture of the provided solution/ every module along with installation and administration guide, which must include High-Level Design (HLD), and Low-Level Design (LLD) along with technical bid. Architecture Diagram of proposed & implemented solution as actual in the Bank environment.
73. The Proposed solution should be free from any kind of vulnerabilities and as and when vulnerabilities are notified by the auditor, Bank, regulators, Govt. of India and any other Govt. agencies, it should be patched within prescribed time with no cost to Bank during the contract period.
74. The bidder shall do regular backup of the solutions as per the defined Banks backup policy and solution should integrate the existing Banks Backup Solution.

Solution Implementation and Migration

The bidder shall coordinate with all solution providers/ vendors while installing and ensure installation and commissioning for running the application.

1. The Bidder shall be responsible to perform a clean uninstall of the existing Antivirus/ endpoint protection solution installed at the endpoints before installation of the new endpoint solution.
2. The bidder shall confirm the integrity of the software supplied i.e., the software is free from bugs, malware, covert channels in code etc. and Integrity certificate should be submitted to the Bank.
3. The production setup and solution architecture including Designing of complete solution, solution Flow architecture and Network Architecture should be designed &

audited by the respective OEM(s)/OSD(s) of the Solution and its components and duly signed by respective OEM before the Final sign-off of the solution.

4. The successful bidder shall migrate all the data from existing EPP, EDR/ATP, XDR & Server Security solution in Bank to new Solutions procured through this RFP.
5. Solution should be able protect applications deployed on Docker, Containers & Virtual cloud for easy, deployment and building on premises if Bank decided to migrate to such setup in future.
6. The Proposed solution should be able to be deployed in Container form bundled into a single package consisting of all libraries, binaries, configuration and all its dependencies. It should be able to run independently irrespective of Operating System (OS) Distribution and underlying physical infrastructure. The bidder shall ensure that container deployment architecture should not limit the application performance, which would be otherwise available in non-container (traditional) deployment.
7. The proposed solution must have redundancy at all levels e.g., network redundancy (for management network interfaces) and power-supply redundancy at hardware/ software level required to achieve the high availability/ redundancy as per defined SLA/uptime.
8. Proposed solutions should have very high-scale architecture on a platform that scales efficiently. The solution should support 64-bit architecture environments for high scalability. Solution should support installation on Windows environment. Solutions should have extensible architecture for easy integration and automation.
9. Solution installation should support multiple-deployment options – Centralized, Distributed and hybrid deployments with option for a centralized operations console view (Dashboard).
10. The Bidder should provide customized (as per the requirement of the Bank) and pre-defined reports in HTML, CSV, Excel, PDF and other required file formats. All reports should be configured to generate auto or scheduled responses and send via SMTP on daily/monthly/yearly as per the Bank requirement at no additional cost to the Bank during the period of contract.
11. The proposed solution should be tightly integrated with all the existing other security tools / setup and new infrastructure /Assets of the Bank.
12. The selected bidder should implement and maintain this Solution for a period of 3 years including, Three (3) years Warranty from the date of final sign-off.

13. For implementation, Bidder should provide resources onsite to complete the implementation on time. A project manager must be deputed onsite during implementation phase at no additional cost to the Bank.
14. The bidders shall also provide the following documents, but not limited to, as part of the deliverables of the project.
    a. Original manuals of all proposed software/applications.
    b. Standard Operating Procedures for various activities such as administration, troubleshooting, regular health check-up, maintenance / clean-up activities etc.
    c. Installation & Technical Master Configuration Documents.
    d. Network & Security Design Documents (Will be approved by the Bank).
    e. Executive summary report for the project to the management fortnightly during implementation till go-live.
    f. Training materials.
15. Data security and Integrity to be ensure at rest as well as in transit.
16. The Bank shall give Bidder/OEM and its personnel only physical access to the support location and the designated hardware & equipment to enable Bidder to provide the maintenance & support services.
17. Bank will provide the Network access / availability for EPP, EDR & Server Security solution integration with Bank network at DR & DR. However, the required network sizing and other details has to be provided by the Bidder.
18. The solution should support the features and functionalities as mentioned in the Compliance to Technical & Functional Specifications of the Solution.

Onsite Technical Support

1. Post implementation the Successful bidder has to ensure the availability of support engineers at Bank's data centre for administration, operations, management and all activities related to the solution on all days of the week as well as beyond office hours, or whenever asked or needed.
2. Resident support engineer shall provide post implementation support at DR site remotely from DC, or visit to that site in case of need, without any additional cost to Bank.
3. Preventive maintenance of devices/ solution should be performed on quarterly basis at all locations for which solution is bought.

4. Overall management of the complete solution such as refinement of policies, creation of policies and database team during Databases creations, etc.
5. Proactive monitoring of health of the solution, including the H/W, S/W, application, solution on various parameters such as CPU, memory, storage, interface utilizations, etc. from Centralize Dashboard.
6. Health check for critical applications\ Workloads
7. Preparing and submitting reports as per the requirement of the Bank. Reports will include daily health monitoring and other statistical reports. If any report is available out of the box, then engineer has to customize the same as per the Bank's requirement with no extra cost to Bank. Engineer may take support from its Backend team and/or OEM if required.
8. Troubleshooting day-to-day issues, faced by end users, pertaining to proposed solution in coordination with Bank's Network integrator, security integrator, desktop management team or other relevant teams/vendors.
9. The Bidder shall provide requisite skilled resources during the implementation period during working hours and for post Implementation, the OTS resource for 24x7x365 from the date of Go-Live. Below are the minimum tentative resources and shift details for OTS (Onsite Technical Support):

Resource Type	Daily working hours	Minimum No. of resources to be present per day
L2	09:00AM to 6:00PM on Bank's Working days. The resources shall be responsible for JK Bank setup and endpoints	1

10. The onsite resources must be on bidder's payroll, subcontracting shall not be allowed of any resource(s) during the contract period.
11. Bidder may deploy additional resources to factor the week-off, leaves, compliance to labour and other applicable laws. Bank shall however bear the cost of the resources as per the quantity mentioned in the Purchase Order only.
12. All the resources deployed should have requisite knowledge and experience required for management and monitoring of the overall operations of all the implemented solutions.

13. Bidder is also required to provide a senior resource as and when required by the Bank, during the entire contract period of 3 years, for managing overall operations of the implemented solutions, without any extra cost to the Bank.
14. Bidder shall also provide one Team Lead for the entire duration of the project who shall be the SPOC for all issues and shall report onsite to the Bank on monthly basis for review.
15. Qualification of resource

Role/ Description	Experience	Educational Qualifications/Certifications/ Skills
L2	Minimum 5 Years	1. Good Communication (written/Oral) 2. Hands-on experience of Endpoint Security Solutions including EPP, EDR, Server Security etc. 3. The resource must be certified professional in the OEM technology.

Training

Bidder(s) must mandatorily provide training to the Bank Core team (Technical & Administrative). It is also the responsibility of the bidder to provide training manuals/SoP to each participant. All training material should be in English and should include Specific architecture and layout done for Bank. Training will be arranged in batches. The training should be provided onsite and remotely.

Upgrades and Updates

1. Bidder should ensure that any signature, patches and virus definition must be updated/installed immediately after release by the OEM/OSD to the solution and integrated endpoints.
2. The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Appliance provided free of cost during contract period. If, however, the upgrades and/or updates are not available or the solution(software) is declared End of Life/ /End of Support, Bidder has to upgrade the solution to an equivalent or higher solution without any additional cost to the Bank

3. The bidder should inform to the Bank if any new version, service pack, upgrade of the proposed solution is released by OEM, within seven (7) days of such release and deploy the upgraded solution and endpoints within 15 days of such release without any cost to the Bank covering all parts, labour and accessories at the respective locations (DC and DR) of the Bank during the period of the contract.
4. During the period of the contract, all upgrades, updates or requirements in hardware, software, licensing, implementation of upgrades, patches, version changes etc., due to whatsoever reason including but not limited to EOL(End-of-Life) or EOS(End-of-Support), shall be done by the bidder within stipulated time but not later than one month without any additional cost to the Bank. EOS/EOL solution will not be accepted and if any solution is declared EOS/EOL during the period of contract, the bidder shall upgrade with equivalent or higher specifications as stated above, at no additional cost to the Bank. The solution Infrastructure (hardware/software or both) provided by the successful bidder should not be declared end of sale within 2 years of sign off of the project. If at all the solution Infrastructure (hardware/software or both) partly or fully, is declared end of sale within 2 years of sign off, the successful bidder has to provide the upgraded version (hardware or both) free of cost, to the Bank. All hardware and software components of complete solution Infrastructure should be updated and maintained by the bidder during the entire tenure of the contract.

Location of Work

The successful bidder shall be required to work in close co-ordination with Bank's teams during entire life cycle of the project. The successful bidder may be required to work at locations prescribed by Bank such as Banks CHQ, DC/DR and other offices as per Banks requirement. All expenses (travelling/lodging, etc.) shall be borne by the successful bidder.

1. **J&K Bank Ltd.**
   Information Security Department / Security Operations Center,
   Corporate Headquarters, M A Road,
   Srinagar 190001, Kashmir (UT of Jammu & Kashmir)
   India

2. **Datacenter Noida**

   Jammu & Kashmir Bank Ltd.
   Facility Management, Noida
   J&K Bank, 5th & 7th Floor, SIFY Green fort

Data Centre, Plot No: B-7, Opposite
Jaypee Hospital, Sector 132, Noida, U.P. India 201301

3. **DR Mumbai**

   Jammu & Kashmir Bank Ltd.
   Disaster Recovery Site,
   Plot. No GEN/72/1/A, TTC Industrial Area
   MIDC Mahape, Navi Mumbai-400701

Invitation for Tender Offer

J&K Bank invites tenders for technical bid (online) and Commercial bid (online) from suitable bidders. In this RFP, the term "bidder / prospective bidder" refers to the bidder delivering products / services mentioned in this RFP.

The prospective bidders are advised to note the following: The interested bidders are required to submit the Non-refundable Application Fees of **₹5000/=** by way of NEFT, details of which are mentioned at clause of Earnest Money Deposit in Part C

1. Representatives of bidders who attend the pre-bid meeting are required to carry an authorization document from the company, an identity card for attending the meeting.

2. Bidders are required to submit Bank guarantee drawn in favor of "J&K BANK LTD" payable at Srinagar, towards Earnest money Deposit (EMD) for **₹ 24, 00,000/- (Twenty-Four Lakh Rupees only)**. The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 6 months from the last date of bid submission and issued by any scheduled commercial Bank acceptable to the Bank. Offers made without EMD will be rejected.

3. Technical Specifications, Price Bid, Terms and Conditions and various formats for submitting the tender offer are described in the tender document and Annexures.

Project Plan

Successful Bidder shall submit the project plan for complete activity as per the Scope of Work detailed in this RFP. This plan should be submitted for review and bank's acceptance within two weeks after the issuance of PO to the successful bidder.

Bank shall issue a Project Plan signoff accepting the same. It shall be the responsibility of the successful bidder to submit and get the plan approved by the Bank authorities within the timelines mentioned above without any delay. Bank shall have the discretion to cancel the purchase order in lieu of delay in submission of the project plan.

Project Milestones & Delivery

The Bank requires the selected bidder to adhere to the agreed delivery milestones of the project. The milestones, along with their associated deliverables and timelines, are outlined in the following table:

If Hardware is applicable

S.NO	Milestones	Weeks from date of issue of P.O.
1.	Contract Execution	2 weeks from date of PO
2.	Delivery of Hardware (if applicable)	8 weeks from date of PO
3.	Installation of licenses, configuration of set-up, Implementation of Policies & complete deployment of solution based on Industry Best Practices.	12 Weeks from date of PO
4.	Payment of Licenses	Yearly in advance based on Actual Consumption of Licenses
5.	Payment of on-site resource	Half-Yearly post rendering of services.

Please note that any of the payments shall be processed only after submission of Performance Bank Guarantee for the project period amounting to 5% of the total project cost.

The bidder must strictly adhere to the project timeline schedule, as specified in the purchase contract executed between the Parties for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the bidder will enable

Bank to resort to any or all of the following provided that the bidder is first given a 30 days written cure period to remedy the breach/delay:

a. Claiming Liquidated Damages

b. Termination of the purchase agreement fully or partly and claim liquidated damages.

c. Forfeiting of Earnest Money Deposit / Invoking EMD Bank Guarantee

However, Bank will have the absolute right to charge penalty and/or liquidated damages as per Tender /contract without giving any cure period, at its sole discretion.

Extension of Delivery Schedule

If, at any time during performance of the Contract, the Bidder should encounter conditions impeding timely delivery, the Bidder shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Bank shall evaluate the situation and may at its discretion extend the Bidder's time for performance against suitable extension of the performance guarantee for delivery.

Non-Delivery

Failure of the successful bidder to comply with the above delivery schedule, shall constitute sufficient grounds for the annulment of the award of contract and invocation of bank guarantee (delivery).

User Acceptance Testing

Successful bidder shall assist Bank in the User Acceptance Testing of the solution for the functionalities stated in this RFP document. Bank shall issue a UAT signoff on successful completion of the UAT. If the UAT fails or there is undue delay of the completion of the UAT due to reasons attributable to the successful bidder, Bank may at its own discretion cancel the purchase order and invoke the Bank guarantee for implementation.

Operationalization of Solution

Bank shall issue Go Live Signoff on successful operationalization of the solution. If there is delay in the operationalization of the solution, Bank reserves the right to cancel the purchase order and invoke the Bank guarantee submitted for implementation.

Review

The solution shall remain under review for a period of 3 months from the date of Go Live Certificate as stated above. The Successful bidder shall be readily available during the review phase for troubleshooting and other support. During the review phase, Bank may request changes to the application as per its requirement and no extra costs shall accrue to the bank for the effort involved in the same. Bank shall issue final acceptance signoff at the end of the review phase.

B-EVALUATION PROCESS

The endeavor of the evaluation process is to fit the best fit Solutions as per the Banks requirement at the best possible price. The evaluation shall be done by the Banks internal committees formed for this purpose. Through this RFP, Bank aims to select a bidder/ application provider who would undertake the J&K Bank maintenance of the required solution. The bidder shall be entrusted with end to end responsibility for the execution of the project under the scope of this RFP. The bidder is expected to commit for the delivery of services with performance levels set out in this RFP in section: Service Level Agreements.

Responses from Bidders will be evaluated in three stages, sequentially, as below:

Stage A. Evaluation of Eligibility

Stage B. Technical Evaluation

Stage C. Commercial Evaluation

The three-stage evaluation shall be done sequentially on knock-out basis. This implies that those Bidders qualifying in Stage A will only be considered for Stage B and those who qualify in Stage B will only be considered for Stage C. Please note that the criteria mentioned in this section are only indicative and Bank, at its discretion, may alter these criteria without assigning any

reasons. Bank also reserves the right to reject any / all proposal(s) without providing any specific reasons. All deliberations and evaluations performed by Bank will be strictly confidential and will be maintained as property of Bank exclusively and will not be available for discussion to any Bidder of this RFP.

JK Bank shall scrutinize the Eligibility bid submitted by the bidder. A thorough examination of supporting documents to meet each eligibility criteria (Annexure D) shall be conducted to determine the Eligible bidders. Bidders not complying with the eligibility criteria are liable to be rejected and shall not be considered for Technical Evaluation.

The bidders meeting the General Eligibility Criteria as per Annexure D will be considered for technical evaluation. Any credential/supporting detail mentioned in "Annexure D – Compliance to Eligibility Criteria" and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a Bidder can provide.

Stage 1 - Evaluation of Eligibility

The Bidders of this RFP will present their responses as detailed in this document. The Response includes details / evidences in respect of the Bidder for meeting the eligibility criteria, leading the Bank to evaluate the Bidder on eligibility criteria. The Bidder will meet the eligibility criteria mentioned in annexure D in this document individually. Bank will evaluate the Bidders on each criterion severally and satisfy itself beyond doubt on the Bidders ability / position to meet the criteria. Those Bidders who qualify on ALL the criteria will only be considered as "Qualified under Stage A" of evaluation and will be considered for evaluation under Stage B. Those Bidders who do not qualify at this Stage A will not be considered for any further processing. The EMD money in respect of such Bidders will be returned on completion of the Stage A evaluation. Bank, therefore, requests that only those Bidders who are sure of meeting all the eligibility criteria only need to respond to this RFP process.

Stage 2 - Evaluation of Technical Bid

All technical bids of bidders who have Qualified Stage A will be evaluated in this stage and a

technical score would be arrived at. The bidder should meet the technical requirements as mentioned in the Annexure E. The Bank will scrutinize the offers to determine their completeness (including signatures from the relevant personnel), errors, omissions in the technical & commercial offers of respective bidders. The Bank plans to, at its sole discretion, waive any minor non- conformity or any minor deficiency in an offer. The Bank reserves the right for such waivers and the Bank's decision in the matter will be final.

Summary of Technical Evaluation Qualification Criteria

- **Total Technical Score: 300 Marks**
- **Minimum Overall Passing Score: 240 Marks (80%)**

Bank may seek clarifications from the any or each bidder as a part of technical evaluation. All clarifications received within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the Bank. Those Bidders who meet the threshold score of **marks** or more will be considered as "Qualified under Stage B" and will be considered for evaluation under Stage C. Those who do not meet the above threshold will not be considered for further evaluation and their EMD monies will be returned.

The bidders will submit the Technical Bid in the format as per Annexure E. A copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the tender document.

Stage 3 - Evaluation of Commercial Bid

The Commercial Bid may be submitted as per the format in Annexure F.

Only those Bidders scoring at least **240 marks out of 300 marks** in the technical evaluation will be short- listed for commercial evaluation.

Once the bidder has complied with the techno functional pre-requisites as mentioned at annexure L and the technical evaluation as mentioned in Annexure E, the bidder shall be eligible for commercial process. The financial proposals will be ranked in terms of their total evaluated cost. The least cost proposal will be ranked as L-1 and the next higher and so on will be ranked as L-2, L-3 etc. The least cost proposal (L-1) will be considered for award of contract.

The bank at its own discretion may undertake reverse auction.

C-RFP SUBMISSION

E-Tendering Process

This RFP will follow e-Tendering Process (e-Bids) as under which will be conducted by Bank's authorized e-Tendering Vendor M/s. e-Procurement Technologies Ltd. through the website ***https://jkbank.abcprocure.com***

a) Vendor Registration
b) Publish of RFP
c) Pre Bid Queries
d) Online Response of Pre-Bid Queries
e) Corrigendum/Amendment (if required)
f) Bid Submission
g) Bids Opening
h) Pre-Qualification
i) Bids Evaluation
j) Reverse Auction with Qualified Bidders
k) Contract Award

Representative of Vendors may contact the Help Desk of e-Tendering agency M/s. e-Procurement Technologies Ltd for clarifications on e-Tendering process:

Service provider:

Service Provider:

M/s. E-procurement Technologies Limited

(Auction Tiger) , B-705, Wall Street- II, Opp. Orient Club, Ellis Bridge, Near Gujarat College,

Ahmedabad- 380006, Gujarat

Help Desk:

Sandhya Vekariya – 6352631968

Ijlalaehmad Pathan – 6352631902

Imran Sodagar - 9328931942

No consideration will be given to e-Bids received after the date and time stipulated and no extension of time will normally be permitted for submission of e-Bids.

Vendors will have to abide by e-Business Rules framed by the Bank in consultation with

M/s. **E-procurement Technologies Limited**

RFP Fees

The RFP application fees may be paid by the bidders through NEFT as per the following details:

Bank Details for RFP Fees	
Account Number	**9931530300000001**
Account Name	**Tender Fee/ Cost Account**
Bank Name	The J&K Bank Ltd
Branch Name	Corporate Headquarters MA Road Srinagar J&K - 190001
IFSC Code	JAKA0HRDCHQ
Amount	INR 5000/=

The Bidder shall solely bear all expenses whatsoever associated with or incidental to the preparation and submission of its Bid and the Bank shall in no case be held responsible or liable for such expenses, regardless of the conduct or outcome of the bidding process including but not limited to cancellation / abandonment / annulment of the bidding process.

Earnest Money Deposit

Prospective bidders are required to submit Bank Guarantee drawn in favor of "Jammu and Kashmir Bank Ltd" payable at Srinagar, towards earnest money deposit (EMD) of INR 24,00,000

(Rupees Twenty-Four Lakh Rupees only). The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 6 months from the last date of bid submission and issued by any scheduled commercial Bank in India (other than Jammu & Kashmir Bank). The Bank will not pay any interest on the EMD. The bidder can also submit the EMD through NEFT as per the following details:

Bank Details for Earnest Money Deposit	
Account Number	**9931070690000001**
Account Name	**Earnest Money Deposit (EMD)**
Bank Name	The J&K Bank Ltd
Branch Name	Corporate Headquarters MA Road Srinagar J&K - 190001
IFSC Code	JAKA0HRDCHQ
Amount	INR **24,00,000**/=

In case of a Bank Guarantee from a Foreign Bank, prior permission of the Bank is essential. The format of Bank Guarantee is enclosed in Annexure G.

EMD submitted through Bank Guarantee/Demand Draft should be physically send in an envelope mentioning the RFP Subject, RFP No. and date to the following address:

Address:	Information Security Department, J&K Bank Ltd. 2nd Floor Annex building , Corporate Headquarters, M. A. Road, Srinagar, J&K Pin-190001

Note: EMD is exempted for all Start-ups as recognized by DPIIT/DIPP.

The EMD made by the bidder will be forfeited if:

a. The bidder withdraws his tender before processing of the same.

b. The bidder withdraws his tender after processing but before acceptance of the PO issued by Bank.

c. The selected bidder withdraws his tender before furnishing an unconditional and irrevocable Performance Bank Guarantee.

d. The bidder violates any of the provisions of the terms and conditions of this tender specification.

The EMD will be refunded to:

a. The Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (other than Jammu & Kashmir Bank) from any scheduled commercial bank in India for 5% of the total project cost for 3 years and valid for 42 months including claim period of 6 months, validity starting from its date of issuance. The PBG shall be submitted within 15 days of the PO issued from the Bank.
b. The Unsuccessful Bidder, only after acceptance of the PO by the selected bidder.

Performance Bank Guarantee (PBG)

The successful bidder will furnish an unconditional performance bank guarantee (other than Jammu & Kashmir Bank) from any scheduled commercial bank in India, for **5%** of the total project cost for **3** years. The format of the PBG is given as per Annexure H. The PBG shall be submitted within **15** days from the date of issuance of Purchase order by the Bank. The PBG shall be denominated in Indian Rupees. All charges whatsoever such as premium, commission etc. with respect to the PBG shall be borne by the Successful Bidder. The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing Bank on the printed letterhead of the issuing Bank. Such forwarding letter shall state that the PBG has been signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of Attorney number and date of execution in his / her favor with authorization to sign the documents. Each page of the PBG must bear the signature and seal of the BG issuing Bank and PBG number. In the event of delays by Successful Bidder in implementation of project beyond the schedules given in the RFP, the Bank may invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation by the Successful Bidder for its failure to complete its obligations under the contract. The Bank shall also be entitled to

make recoveries from the Successful Bidder's bills, Performance Bank Guarantee, or any other amount due to him, the equivalent value of any payment made to him by the Bank due to inadvertence, error, collusion, misconstruction or misstatement. The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Successful Bidder under the contract. However, no interest shall be payable on the PBG.

Tender Process

i. Three-stage bidding process will be followed. The response to the tender should be submitted in three parts: Eligibility, Technical Bid and Commercial Bid through online e-tendering portal with a tender document fee mentioned.

ii. The Bidder shall submit their offers strictly in accordance with the terms and conditions of the RFP. Any Bid, which stipulates conditions contrary to the terms and conditions given in the RFP, is liable for rejection. Any decision of Bank in this regard shall be final, conclusive and binding on the Vendor.

iii. L1 vendor will be arrived at through Online Reverse Auction (ORA). After ORA, if there is a large variance in the prices quoted, Bank reserves the right to call the successful bidder for a price negotiation.

iv. On conclusion of ORA, the Successful Bidder (L1) shall submit to the Bank the price breakup for the ORA amount in the format as provided by the Bank. If the price breakup is not submitted commercial offers, bank to the Bank within 3 days from the date of the ORA, the Bank reserve the right to cancel the further processing of the bid.

v. Bank will enter in to contract with the L1 bidder (in normal cases). Rates fixed at the time of contract will be non-negotiable for the whole contract/SLA period and no revision will be permitted. This includes changes in taxes or similar government decisions.

vi. In normal course L1 vendor will get 100% of the work order. However, the Bank reserves the right to distribute the work among the shortlisted firms if required, keeping in view their performance, relative strengths and operational convenience. Therefore, the

lowest tendering firm shall not have sole claim over the entire order. The L1-rate Vendor will get at least 50% of the work contract and the remaining work orders will be may be given to L2 and/or L3 rate vendor, provided they accept the L1 Rates. Vendors of L4 rate and beyond will not be considered. Bank's decision in this regard will be final.

vii. This contract will be awarded for a period of 3 years from date of signing the AMC contract. It may be further renewed if both parties wish to continue on the same terms of service.

viii. If the service provided by the vendor is found to be unsatisfactory or if at any time it is found that the information provided by the vendor is false, the Bank reserves the right to revoke the awarded contract without giving any notice to the vendor. Bank's decision in this regard will be final.

ix. If any of the shortlisted Vendors are unable to fulfil the orders within the stipulated period, then the Bank will have the right to allot those unfulfilled orders to other participating vendors after giving 30-days" notice to the defaulting Vendor. Also, during the period of the AMC contract due to unsatisfactory service to our branches/offices, Bank will have the right to cancel the contract and award the contract to other participating vendors.

Bidding Process

i. The bids in response to this RFP must be submitted in three parts:
   a. Confirmation of Eligibility Criteria
   b. Technical Bid" (TB) including and
   c. Commercial Bid" (CB).

ii. The mode of submission of Confirmation of Eligibility Criteria, Technical Bid (TB) and Commercial Bid (CB) shall be online.

iii. Bidders are permitted to submit only one Technical Bid and relevant Commercial Bid. More than one Technical and Commercial Bid should not be submitted.

iv. The Bidders who qualify the Eligibility Criteria & Technical Evaluation will be qualified for commercial bid evaluation. The successful Bidder will be determined based on the Lowest Commercial Quote (L1) after reverse auction as per the stated Commercial Evaluation process.

v. Receipt of the bids shall be closed as mentioned in the bid schedule. Bid received after the scheduled closing time will not be accepted by the Bank under any circumstances.

vi. Earnest Money Deposit must accompany all tender offers as specified in this tender document. EMD amount / Bank Guarantee in lieu of the same should accompany the Technical Bid. Bidders, who have not paid Cost of RFP and Security Deposit (EMD amount) will not be permitted to participate in the bid and bid shall be summarily rejected.

vii. All Schedules, Formats, Forms and Annexures should be stamped and signed by an authorized official of the bidder'.

viii. The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of a bid not substantially responsive to the bidding documents in every respect will be at the bidder's risk and may result in rejection of the bid.

ix. No rows or columns of the tender should be left blank. Offers with insufficient information are liable to rejection.

x. The bid should contain no interlineations, erasures or over-writings except as necessary to correct errors made by the bidder. In such cases, the person/s signing the bid should initial such corrections.

xi. Bank reserves the right to re-issue / re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of the Bank in this regard shall be final, conclusive and binding on the Bidder.

xii. Modification to the Bid Document, if any, will be made available as an addendum/corrigendum on the Bank's website and Online tendering portal.

xiii. All notices regarding corrigenda, addenda, amendments, time-extension, clarification, response to bidders' queries etc., if any to this RFP, will not be published through any advertisement in newspapers or any other mass media. Prospective bidders shall regularly visit Bank's website or online tendering portal to get themselves updated on changes / development in relation to this RFP.

xiv. Prices quoted should be exclusive of GST.

xv. Applicable taxes would be deducted at source, if any, as per prevailing rates.

xvi. The price ("Bid Price") quoted by the Bidder cannot be altered or changed due to escalation on account of any variation in taxes, levies, and cost of material.

xvii. During the period of evaluation, Bidders may be asked to provide more details and explanations about information they have provided in the proposals. Bidders should respond to such requests within the time frame indicated in the letter/e-mail seeking the explanation.

xviii. The Bank's decision in respect to evaluation methodology and short-listing Bidders will be final and no claims whatsoever in this respect will be entertained.

xix. The Bidder shall bear all the costs associated with the preparation and submission of its bid and the bank, will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

Deadline for Submission of Bids

i. Bids must be received at the portal and by the date and time mentioned in the "Schedule of Events".

ii. In case the Bank extends the scheduled date of submission of Bid document, the Bids shall be submitted at the portal by the time and date rescheduled. All rights and obligations of the Bank and Bidders will remain the same.

iii. Any Bid received after the deadline for submission of Bids prescribed at the portal, will be rejected.

Bid Validity Period

i. Bid shall remain valid for duration of 06 calendar months from Bid submission date.

ii. Price quoted by the Bidder in Reverse auction shall remain valid for duration of 6 calendar months from the date of conclusion of RA.

iii. Once Purchase Order or Letter of Intent is issued by the Bank, the said price will remain fixed for the entire Contract period and shall not be subjected to variation on any account, including exchange rate fluctuations and custom duty. A Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

Bid Integrity

Willful misrepresentation of any fact within the Bid will lead to the cancellation of the contract without prejudice to other actions that the Bank may take. All the submissions, including any accompanying documents, will become property of the Bank. The Bidders shall be deemed to license, and grant all rights to the Bank, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements.

Cost of Bid Document

The participating Bidders shall bear all the costs associated with or relating to the preparation and submission of their Bids including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstration or presentations which may be required by the Bank or any other costs incurred in connection with or relating to their Bid. The Bank shall

not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder regardless of the conduct or outcome of the bidding process.

Contents of Bid Document

i. The Bidder must thoroughly study/analyse and properly understand the contents of this RFP, its meaning and impact of the information contained therein.

ii. Failure to furnish all information required in this RFP or submission of Bid not responsive to this RFP in any respect will be at the Bidder's risk and responsibility and the same may finally result in rejection of its Bid. The Bank has made considerable effort to ensure that accurate information is contained in this RFP and is supplied solely as guidelines for Bidders.

iii. The information provided by the Bidders in response to this RFP will become the property of the Bank and will not be returned. Incomplete information in Bid document may lead to non-consideration of the proposal.

iv. The Bid prepared by the Bidder, as well as all correspondences and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature shall be submitted in English.

Modification and Withdrawal of Bids

i. The Bidder may modify or withdraw its Bid after the Bid's submission, provided that written notice of the modification, including substitution or withdrawal of the Bids, is received at the portal, prior to the deadline prescribed for submission of Bids.

ii. No modification in the Bid shall be allowed, after the deadline for submission of Bids.

iii. No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified in this RFP. Withdrawal of a Bid during this interval may result in the forfeiture of EMD submitted by the Bidder.

Payment Terms

The Bidder must accept the payment terms proposed by the Bank as proposed in this section.

The Payments shall be made on the achievement of the following project milestones:

Project Milestone	Payment (Incl. Of applicable taxes)
On delivery of Hardware (If applicable)/ Installation of EDR with Advanced XDR Capabilities Solution and followed by activation of licenses subject to receiving UAT sign off & confirmation from JK Bank	100% of Hardware Cost (If Applicable) 40% of First year License cost
On Deploying policies and post Go Live Sign off as per JK Bank's requirement	60% of First year License cost
Payments shall be made for 2nd & 3rd Year	100% Yearly in advance based on Actual Consumption of Licenses

***All Payments will be done post confirmation from the Bank Teams.**

Payment terms: -

1. Rates to be quoted exclusive of GST. The quantity mentioned above is indicative only and the actual number may change based on assessment of business requirements of the Bank.

2. Invoices to be raised after submission of 5% PBG of the total project cost & execution of NDA & SLA with the Bank.

3. Sign off from Bank at various stages.

All other terms and conditions as per RFP.

D-GENERAL TERMS & CONDITIONS

Standard of Performance

The bidder shall perform the service(s) and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and

practices used in industry and with professional engineering standards recognized by the international professional bodies and shall observe sound management, technical and engineering practices. It shall employ appropriate advanced technologies, procedures and methods. The Bidder shall always act, in respect of any matter relating to the Contract, as faithful advisors to J&K Bank and shall, at all times, support and safeguard J&K Bank's legitimate interests.

Indemnity

The Successful bidder shall indemnify and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings (including attorney fees), relating to or resulting from: -

i. Intellectual Property infringement or misappropriation of any third-party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.

ii. Claims made by the employees who are deployed by the Successful bidder.

iii. Breach of confidentiality obligations by the Successful bidder,

iv. Negligence (including but not limited to any acts or omissions of the Successful bidder, its officers, principals or employees) or misconduct attributable to the Successful bidder or any of the employees deployed for the purpose of any or all of the its obligations,

v. Any loss or damage arising out of loss of data;

vi. Bonafide use of deliverables and or services provided by the successful bidder;

vii. Non-compliance by the Successful bidder with applicable laws/Governmental/ Regulatory Requirements.

The Successful bidder shall be responsible for any loss of data, loss of life etc. due to acts of its representatives, and not just arising out of negligence or misconduct, as such liabilities pose significant risk.

It is hereby agreed that the above said indemnity obligations shall apply notwithstanding anything to the contrary contained in this Tender document and subsequent Agreement and shall survive the termination of the agreement for any reason whatsoever. The Successful bidder will have sole control of its defence and all related settlement negotiations.

Cancellation of Contract and Compensation

The Bank reserves the right to cancel the contract of the selected Bidder and recover expenditure incurred by the Bank on the following circumstances. The Bank would provide 30 days' notice to rectify any breach/ unsatisfactory progress:

a. The selected Bidder commits a breach of any of the terms and conditions of the RFP/contract.

b. The selected Bidder becomes insolvent or goes into liquidation voluntarily or otherwise.

c. Delay in completion of Supply, Installation of Project Deliverables.

d. Serious discrepancies noted in the inspection.

e. Breaches in the terms and conditions of the Order.

f. Non submission of acceptance of order within 7 days of order.

g. Excessive delay in execution of order placed by the Bank.

h. The progress regarding execution of the contract, made by the selected Bidder is found to be unsatisfactory.

i. If the selected Bidder fails to complete the due performance of the contract in accordance with the agreed terms and conditions.

Liquidated Damages

If bidder fails to perform services within stipulated time schedule, the Bank shall, without prejudice to its other remedies under the contract, deduct from the contract price, as

liquidated damages, a sum equivalent to 1% of the total project cost for delay of each week or part thereof maximum up to 10% of contract price. Once the maximum is reached, Bank may consider termination of Contract pursuant to the conditions of contract. However, the bank reserves the right to impose / waive any such penalty.

Fixed Price

The Commercial Offer shall be on a fixed price basis, inclusive of all taxes and levies (excluding GST). No price increases due to increases in customs duty, excise, tax, dollar price variation etc. will be permitted.

Right to Audit

"Bank reserves the right to conduct an audit/ ongoing audit of the Company/Service Provider(including its sub-contractors).The Company shall be subject to annual audit by internal/ external Auditors appointed by the Bank / inspecting official from the RBI or the persons authorized by RBI or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and company is required to submit such certification by such Auditors to the Bank.

Company shall allow the Bank and RBI or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Company within a reasonable time failing which Company will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank."

Force Majeure

i. The Selected Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

ii. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractors fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, pandemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.

iii. Unless otherwise directed by the Bank in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

iv. In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and the contractor shall hold consultations in an endeavor to find a solution to the problem.

v. Notwithstanding above, the decision of the Bank shall be final and binding on the successful bidder regarding termination of contract or otherwise.

Publicity

Bidders, either by itself or through its group companies or Associates, shall not use the name and/or trademark/logo of Bank, in any sales or marketing publication or advertisement, or in any other manner.

Amendments

Any provision of hereof may be amended or waived if, and only if such amendment or waiver is in writing and signed, in the case of an amendment by each Party, or in the case of a waiver,

by the Party against whom the waiver is to be effective.

Assignment

The Selected Bidder shall not assign, in whole or in part, the benefits or obligations of the contract to any other person without the prior written consent of the Bank. However, the Bank may assign any of its rights and obligations under the Contract to any of its affiliates without prior consent of Bidder.

Severability

If any provision of this agreement or any document, if any, delivered in connection with this agreement is partially or completely invalid or unenforceable in any jurisdiction, then that provision shall be ineffective in that jurisdiction to the extent of its invalidity or unenforceability. However, the invalidity or unenforceability of such provision shall not affect the validity or enforceability of any other provision of this Agreement, all of which shall be construed and enforced as if such invalid or unenforceable provision was/were omitted, nor shall the invalidity or unenforceability of that provision in one jurisdiction affect its validity or enforceability in any other jurisdiction. The invalid or unenforceable provision will be replaced in writing by a mutually acceptable provision, which being valid and enforceable comes closest to the intention of the Parties underlying the invalid or unenforceable provision.

Applicable law and jurisdictions of court

The Contract with the selected Bidder shall be governed in accordance with the Laws of UT Of J&K read with laws of India so far as they are applicable to the UT of J&K for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Srinagar (with the exclusion of all other Courts). However, the services from the bidder during the period of dispute or pending resolution shall continue as far as is reasonably practical.

Resolution of Disputes and Arbitration clause

The Bank and the Bidder shall make every effort to resolve any disagreement or dispute amicably, arising in connection with the Contract, by direct and informal negotiation between the designated Officer of the Bank for …….. and designated representative of the Bidder. If designated Officer of the Bank and

representative of Bidder are unable to resolve the dispute within reasonable period, which in any case shall not exceed 30 days, they shall immediately escalate the dispute to the senior authorized personnel designated by the Bank and Bidder respectively. If even after elapse of reasonable period, which in any case shall not exceed 30 days, the senior authorized personnel designated by the Bank and Bidder are unable to resolve the dispute amicably OR any party fails to designate its officer/representative/ senior authorized personnel within 30 days from the date of request in writing for the same by the other party for amicable settlement of dispute, the same shall be referred to a sole arbitrator to be appointed by Bank. The Arbitration and Conciliation Act, 1996 will be applicable to the arbitration proceeding and the venue of the arbitration shall be at Srinagar. The language of the arbitration proceedings shall be in English. The award of the arbitrator shall be final and binding. The courts at Srinagar shall have exclusive jurisdiction at Srinagar.

Execution of Service Level Agreement (SLA)/ Non-Disclosure Agreement (NDA)

The Successful Bidder shall have to execute service level agreement for deliverables and successful execution of the projects to meet Banks requirement to its satisfaction. The Bank would stipulate strict penalty clauses for nonperformance or any failure in the implementation/efficient performance of the project. The Bidder should execute the Agreement within 7 days from the date of acceptance of Work Order. The date of agreement shall be treated as date of engagement and the time-line for completion of the assignment shall be worked out in reference to this date. The Bidder hereby acknowledges and undertakes that terms and conditions of this RFP may be varied by the Bank in its absolute and sole discretion. The SLA/NDA to be executed with the successful bidder shall accordingly be executed in accordance with such varied terms.

'NO CLAIM' Certificate

The Bidder shall not be entitled to make any claim(s) whatsoever, against J&K Bank, under or by virtue of or arising out of, the Contract/Agreement, nor shall J&K Bank entertain or consider any such claim, if made by the Bidder after he has signed a 'No Claim' Certificate in favor of J&K Bank in such form as shall be required by J&K Bank after the works are finally accepted.

Cost and Currency

The Offer must be made in Indian Rupees only, including the following:

a) Cost of the equipment/software/licenses specified
b) Installation, commissioning, maintenance, migration charges, hosting charges, if any,
c) Comprehensive on-site software support.
d) Packing, Forwarding and Transportation charges up to the sites to be inclusive.
e) All taxes and levies are for Destinations.
f) Bidder have to make their own arrangements for obtaining road permits wherever needed.

No Agency

The Service(s) of the Bidder herein shall not be construed as any agency of J&K Bank and there shall be no Principal - Agency relationship between J&K Bank and the Bidder in this regard.

Project Risk Management

The selected bidder shall develop a process & help Bank to identify various risks, threats & opportunities within the project. This includes identifying, analyzing & planning for potential risks, both positive & negative, that might impact the project & minimizing the probability of & impact of positive risks so that project performance is improved for attainment of business goals.

Information Security

a. The Successful Bidder and its personnel shall not carry any written material, layout, diagrams, hard disk, flash / pen drives, storage tapes or any other media out of J&K Bank's premises without written permission from J&K Bank.

b. The Successful Bidder's personnel shall follow J&K Bank's information security policy and instructions in this regard.

c. The Successful Bidder acknowledges that J&K Bank 's business data and other proprietary information or materials, whether developed by J&K Bank or being used by J&K Bank pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to J&K Bank; and the

Successful Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Successful Bidder to protect its own proprietary information. Successful Bidder recognizes that the goodwill of J&K Bank depends, among other things, upon the Successful Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Successful Bidder could damage J&K Bank. By reason of Successful Bidder's duties and obligations hereunder, Successful Bidder may come into possession of such proprietary information, even though the Successful Bidder does not take any direct part in or furnish the Service(s) performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by the Contract/Agreement. Successful Bidder shall use such information only for the purpose of performing the Service(s) under the Contract/Agreement.

d. Successful Bidder shall, upon termination of the Contract/Agreement for any reason, or upon demand by J&K Bank, whichever is earliest, return any and all information provided to Successful Bidder by J&K Bank, including any copies or reproductions, both hardcopy and electronic.

e. That the Successful Bidder and each of its subsidiaries have taken all technical and organizational measures necessary to protect the information technology systems and Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses. Without limiting the foregoing, the Successful Bidder and its subsidiaries have used reasonable efforts to establish and maintain, and have established, maintained, implemented and complied with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses.

f. The Successful Bidder shall certify that to the knowledge of the Successful Bidder, there has been no security breach or other compromise of or relating to any information technology and computer systems, networks, hardware, software, data, or equipment owned by the Successful Bidder or its subsidiaries or of any data of the Successful Bidder's, the Operating Partnership's or the Subsidiaries' respective customers, employees, suppliers, vendors that they maintain or that, to their knowledge, any third party maintains on their behalf (collectively, "IT Systems and Data") that had, or would reasonably be expected to have had, individually or in the aggregate, a Material Adverse Effect, and

g. That the Successful Bidder has not been notified of, and has no knowledge of any event or condition that would reasonably be expected to result in, any security breach or other compromise to its IT Systems and Data;

h. That the Successful Bidder is presently in compliance with all applicable laws, statutes, rules or regulations relating to the privacy and security of IT Systems and Data and to the protection of such IT Systems and Data from unauthorized use, access, misappropriation or modification. Besides the Successful Bidder confirms the compliance with Banks Supplier Security Policy.

i. That the Successful Bidder has implemented backup and disaster recovery technology consistent with generally accepted industry standards and practices.

j. That the Successful Bidder and its subsidiaries IT Assets and equipment, computers, Systems, Software's, Networks, hardware, websites, applications and Databases (Collectively called IT systems) are adequate for, and operate and perform in all material respects as required in connection with the operation of business of the Successful Bidder and its subsidiaries as currently conducted, free and clear of all material bugs, errors, defects, Trojan horses, time bombs, malware and other corruptants.

k. That the Successful Bidder shall be responsible for establishing and maintaining an information security program that is designed to:

   - Ensure the security and confidentiality of Customer Data, Protect against any

anticipated threats or hazards to the security or integrity of Customer Data, and

- That the Successful Bidder will notify Customer of breaches in Successful Bidder's security that materially affect Customer or Customer's customers. Either party may change its security procedures from time to time as commercially reasonable to address operations risks and concerns in compliance with the requirements of this section.

l. The Successful Bidder shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of Personal Data and/or use, access, copying, exhibition, transmission or removal of Bank's Confidential Information from Companies facilities. Successful Bidder shall promptly provide Bank with written descriptions of such procedures and policies upon request. Bank shall have the right, upon reasonable prior written notice to Successful Bidder and during normal business hours, to conduct on-site security audits or otherwise inspect Companies facilities to confirm compliance with such security requirements.

m. That Successful Bidder shall establish and maintain environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss or alteration of the Client Data, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are no less rigorous than those maintained by Successful Bidder for its own information or the information of its customers of a similar nature.

n. That the Successful Bidder shall perform, at its own expense, a security audit no less frequently than annually. This audit shall test the compliance with the agreed-upon security standards and procedures. If the audit shows any matter that may adversely affect Bank, Successful Bidder shall disclose such matter to Bank and provide a detailed plan to remedy such matter. If the audit does not show any matter that may adversely affect Bank, Bidder shall provide the audit or a reasonable summary thereof to Bank. Any such summary may be limited to the extent necessary to avoid a breach of Successful Bidder's security by virtue of providing such summary.

o. That Bank may use a third party or its own internal staff for an independent audit or to monitor the Successful Bidder's audit. If Bank chooses to conduct its own security audit, such audit shall be at its own expense. Successful Bidder shall promptly correct any deficiency found in a security audit.

p. That after providing 30 days prior notice to Successful Bidder, Bank shall have the right to conduct a security audit during normal business hours to ensure compliance with the foregoing security provisions no more frequently than once per year. Notwithstanding the foregoing, if Bank has a good faith belief that there may have been a material breach of the agreed security protections, Bank shall meet with Successful Bidder to discuss the perceived breach and attempt to resolve the matter as soon as reasonably possible. If the matter cannot be resolved within a thirty (30) day period, the parties may initiate an audit to be conducted and completed within thirty (30) days thereafter. A report of the audit findings shall be issued within such thirty (30) day period, or as soon thereafter as is practicable. Such audit shall be conducted by Successful Bidder's auditors, or the successors to their role in the event of a corporate reorganization, at Successful Bidder's cost.

q. Successful Bidders are liable for not meeting the security standards or desired security aspects of all the ICT resources as per Bank's IT/Information Security / Cyber Security Policy. The IT /Information Security/ Cyber Security Policy will be shared with successful Bidder. Successful Bidders should ensure Data Security and protection of facilities/application managed by them.

r. The deputed persons should aware about Bank's IT/IS/Cyber security policy and have to maintain the utmost secrecy & confidentiality of the bank's data including process performed at the Bank premises. At any time, if it comes to the notice of the bank that data has been compromised / disclosed/ misused/misappropriated then bank would take suitable action as deemed fit and selected vendor would be required to compensate the bank to the fullest extent of loss incurred by the bank. Besides bank will be at liberty to blacklist the bidder and take appropriate legal action against bidder.

s. The Bank shall evaluate, assess, approve, review, control and monitor the risks and materiality of vendor/outsourcing activities and Successful Bidder shall ensure to support baseline system security configuration standards. The Bank shall also conduct effective due

diligence, oversight and management of third-party vendors/service providers & partners.

t. Vendor criticality assessment shall be conducted for all partners & vendors. Appropriate management and assurance on security risks in outsources and partner arrangements shall be ensured.

Survival

Any provision of the Contract/Agreement which, either expressly or by implication, survives the termination or expiration of the Contract/Agreement, shall be complied with by the Parties including that of the provisions of indemnity, confidentiality, non- disclosure in the same manner as if the present Contract/Agreement is valid and in force and effect. The provisions of the clauses of the Contract/Agreement in relation to Documents, data, processes, property, Intellectual Property Rights, indemnity, publicity and confidentiality and ownership shall survive the expiry or termination of the Contract/Agreement and in relation to confidentiality, the obligations continue to apply unless J&K Bank notifies the Bidder of its release from those obligations.

No Set-Off, Counter-Claim and Cross Claims

In case the Bidder has any other business relationship(s) with J&K Bank, no right of set-off, counter-claim and cross-claim and or otherwise will be available under this Contract/Agreement to the Bidder for any payment's receivable under and in accordance with that business.

Statutory Requirements

During the tenure of the Contract/Agreement nothing shall be done by the Bidder in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof governing inter-alia customs, foreign exchange, etc., and the Bidder shall keep J&K Bank, its directors, officers, employees, representatives, agents and consultants indemnified in this regard.

Bidder Utilization of Know-how

J&K Bank will request a clause that prohibits the finally selected bidder from using any information or know-how gained in this contract for another organization whose business activities are similar in part or in whole to any of those of the Bank anywhere in the world without prior written consent of the Bank during the period of the contract and one year thereafter.

Corrupt and Fraudulent practice

i. It is required that Company observe the highest standard of ethics during the procurement and execution of such contracts and not to indulge in any corrupt and fraudulent practice.

ii. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.

iii. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

iv. The Bank reserves the right to reject a proposal for award if it determines that the Company recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

v. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it becomes known that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

Solicitation of Employees

Bidder will not hire employees of J&K Bank or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of the J&K Bank directly involved in this contract during the period of the contract and one year thereafter.

Proposal Process Management

The Bank reserves the right to accept or reject any/all proposal/ to revise the RFP, to request one or more re-submissions or clarifications from one or more BIDDERs, or to cancel the process in part or whole. No BIDDER is obligated to respond to or to continue to respond to the RFP. Additionally, the Bank reserves the right to alter the requirements, in part or whole, during the RFP process. Each party shall be entirely responsible for its own costs and expenses that are incurred while participating in the RFP, subsequent presentation and contract negotiation processes.

Confidentiality Provision

The bidder shall hold in confidence all the information, documentation, etc. which shall come to their knowledge (Confidential Information) and shall not disclose or divulge confidential information to any third party or use Confidential Information or any part thereof without written consent of the Bank.

Confidential Information means information which is by its nature confidential or is designated by the bank and confidential information and includes:

i. All information marked or otherwise designated as confident.

ii. Information which relates to the financial position, the internal management structure, the Personnel, policies and strategies of the Bank

iii. Data of the bank, customer lists, customer information, account information, and business information regarding business planning and operation of the Bank or otherwise information or data whether such data is permanent or otherwise.

The restriction imposed in this clause does not apply to any disclosure or information:

i. Which at the material time was in public domain other than breach of this clause; or

ii. Which is required to be disclosed on account of order of any competent court or tribunal provided that while disclosing any information, Bank shall be informed about the same vide prior notice unless such notice is prohibited by applicable law.

Sub-Contracting

The services offered to be undertaken in response to this RFP shall be undertaken to be provided by the bidder/ directly employing their employees, and there shall not be any sub-contracting. All the resources deployed by the bidder should be on the bidder's payroll.

Reverse Auction

In order to reduce the time involved in the procurement process, Bank shall be entitled to complete the entire procurement process through a single Reverse Auction or in multiple Reverse Auctions. The Bank shall however, be entitled to cancel the Reverse Auction process, if in its view procurement or Reverse Auction process cannot be conducted in a fair manner and / or in the interest of the Bank.

Award Notification

The Bank will award the contract to the successful Bidder, out of the Bidders who have responded to Bank's tender as referred above, who has been determined to qualify to perform the contract satisfactorily, and whose Bid has been determined to be substantially responsive, and is the lowest commercial Bid.

The Bank reserves the right at the time of award of contract to increase or decrease of the quantity or change in location where services are required from what was originally specified while floating the tender without any change in unit price or any other terms and conditions.

Suspension of Work

The Bank reserves the right to suspend and reinstate execution of the whole or any part of the work without invalidating the provisions of the contract. The Bank will issue orders for suspension or reinstatement of the work to the Successful Bidder in writing. The time for completion of the work will be extended suitably to account for duration of the suspension.

Penalty for non-delivery

If the Bidder does not deliver, as per the project milestone delivery schedule, or such authorized extension of delivery period as may be permitted in writing by Bank, Bank shall impose a penalty as given below:

Penalty at the rate of 2% of the total purchase order value for each week's delay beyond the stipulated delivery period subject to a maximum of 10%.

Taxes and Duties

a. Successful Bidder will be entirely responsible for all duties, levies, imposts, costs, charges, license fees, road permit etc, in connection with delivery of equipment at site including incidental services and commissioning.

b. Income/Corporate taxes in India: The Successful Bidder shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India

c. Tax Deduction at Source: Wherever the laws and regulations require deduction of such taxes at source of payment, Bank shall affect such deductions from the payment due to the Successful Bidder. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by Bank as per the laws and regulations in force. Nothing in the Contract shall relieve the Successful Bidder from his responsibility to pay any tax that may be levied in India on income and profits made by Successful Bidder in respect of this contract.

d. The Bank shall if so required by applicable laws in force, at the time of payment, deduct income tax payable by the Successful Bidder at the rates in force, from the amount due to the Successful Bidder and pay to the concerned tax authority directly.

Annexure A: Confirmation of Terms and Conditions

To

Chief Information Security Officer

Information Security Department.

Corporate Headquarters

The Jammu & Kashmir Bank M.A. Road, Srinagar,

190 001 J&K.

Dear Sir,

Sub: RFP No ……. For Selection of vendor for Endpoint Detection & Response (EDR) solution with Advanced XDR Capabilities ……. ……. date ……

Further to our proposal dated ....., in response to the Request for Proposal for selection of vendor for Endpoint Detection & Response (EDR) solution with Advanced XDR Capabilities (hereinafter referred to as "RFP") issued by The Jammu & Kashmir Bank (J&K BANK) we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations, payment terms, scope, SLAs etc. as contained in the RFP and the related addendums and other documents issued by the Bank.

Place:

Date: Seal and signature of the bidder

Annexure B: Tender Offer Cover Letter

To
Chief Information Security Officer
Information Security Department.
Corporate Headquarters
The Jammu & Kashmir Bank M.A. Road, Srinagar,
190 001 J&K.

Dear Sir,

Sub: RFP no: _____ for selection of vendor for Endpoint Detection & Response (EDR) solution with Advanced XDR Capabilities at locations i.e. Primary Data Centre and Disaster Recovery Site **dated _____**

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer to _____to Bank as mentioned in RFP document in conformity with the said tender documents in accordance with the Commercial bid and made part of this tender.

We understand that the RFP provides generic specifications about all the items and it has not been prepared by keeping in view any specific bidder.

We understand that the RFP floated by the Bank is a confidential document and we shall not disclose, reproduce, transmit or made available it to any other person.

We have read, understood and accepted the terms/ conditions/ rules mentioned in the RFP including the conditions applicable to reverse auction proposed to be followed by the Bank.

Until a formal contract is prepared and executed, this tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us.

We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India and the UT of J&K.

We have never been barred/black-listed by any regulatory / statutory authority in India.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We certify that we have provided all the information requested by the Bank in the format

requested for. We also understand that the Bank has the exclusive right to reject this offer in case the Bank is of the opinion that the required information is not provided or is provided in a different format. It is also confirmed that the information submitted is true to our knowledge and the Bank reserves the right to reject the offer if anything is found incorrect.

Place:

Date:

Seal and signature of the bidder

Annexure C: Details of SI/OEM

Details filled in this form must be accompanied by sufficient documentary evidence, in order to facilitate the Bank to verify the correctness of the information.

S. No.	PARTICULARS	DETAILS
1	Name of the Company	
2	Postal Address	

3	Telephone / Mobile / Fax Numbers	
4	Constitution of Company	
5	Name & Designation of the Person Authorized to make commitments to the Bank	
6	Email Address	
7	Year of Commencement of Business	
8	Sales Tax Registration No	
9	Income Tax PAN No	
10	Service Tax / GST Registration No	
11	Whether OEM or System Integrator	
12	Name & Address of OEM/s.	
13	Brief Description of after sales services facilities available with the SI/OEM	
14	Web Site address of the Company	

Date:

Seal and signature of the bidder

Annexure D: Compliance to Eligibility Criteria

The bidder needs to comply with all the eligibility criteria mentioned below. Non-compliance to any of these criteria would result in outright rejection of the Bidder's proposal. The bidder is expected to provide proof for each of the points for eligibility evaluation criteria. Any credential detail not accompanied by required relevant proof documents will not be

considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

The decision of the Bank would be final and binding on all the Bidders to this document. The Bank may accept or reject an offer without assigning any reason what so ever.

The bidder must meet the following criteria to become eligible for bidding:

S. No	Financial and other Requirement to be met by the Bidder	Supporting Documents to be submitted	Bidder's Compliance (Yes / No)
1	• The Bidder company should be an Indian firm / company or a multi-national company having a valid license to operate in India for its activity. • The Bidder should be registered as a company (as defined in the Companies Act, 2013) or as a partnership firm (registered under section 59 of the Partnership Act, 1932) or as a limited liability partnership (under the Limited Liability Partnership Act, 2008). • The Bidder should be in operation for at least five (05) years as on date of RFP. (*DPIIT recognized start-ups exempted*)	• Certificate of Incorporation if it is company. • Partnership deed along with tax returns if it is a partnership firm or limited liability partnership. • GST certificate along with PAN Card copy if it is a proprietary firm.	
2	The Bidder should have minimum annual turnover of Rs 100 crore or more	Copy of the audited Balance Sheet and Certificate of the	

	during the last 3 Financial years 2022-23 & 2023-24 & 2024-25. (Micro and Small enterprises - MSEs and DPIIT recognized start-ups are exempted from this clause).	Chartered Accountant for last three years.	
3	The Bidder should have positive net worth as per audited Balance sheet of the FY 2022-23 & 2023-24 & 2024-25.	Certificate of the Chartered Accountant for the last three years along with P&L Statements.	
4	Bidders shall be the Original Equipment Manufacturers (OEM) of Solution (OR) An authorized System Integrator.	If the applicant is an OEM, an Undertaking Letter has to be submitted in this effect. If the bidder is an Authorized System Integrator, an Authorization letter from their OEM to deal / market their product in India and it should be valid at the time of submission of the Bid	
5	The OEM must have a proven track record of at least three successful deployments in BFSI sector with minimum deployment of 20,000 licenses. One of the deployments must be in scheduled commercial bank in the past three years.	Client references and contact details (email / landline / mobile) of customers for whom the Bidder has provided the services. Work orders to be submitted with Start and End Date of the Project to be mentioned.	
6	The bidder must have a proven track record of at least one successful deployment in BFSI sector with minimum deployment of 20,000 licenses.	Client references and contact details (email / landline / mobile) of customers for whom the Bidder has provided the services.	

		Work orders to be submitted with Start and End Date of the Project to be mentioned.	
7	The Bidder should not be involved in any Bankruptcy filing or for protection from it.	Undertakings from the bidder in this regard should be enclosed.	
8	The Bidder should not be a blacklisted by any Government / PSU department or bank.	Undertakings from the bidder in this regard should be enclosed.	
9	The bidder must have at least 3 certified resources from OEM technology with highest certification.	Copy of Certificate	
10	The bidder must place one resource in Banks DC. The resource must be certified professional in the OEM technology.	Copy of Certificate	

Please enclose documentary proof for all the above criteria. In absence of these, the bids will not be considered for further evaluation. No further correspondence will be entertained in this case. The Bank reserves the right to verify/evaluate the claims made by the vendor independently. Any misrepresentation will entail rejection of the offer.

Note: Please write description of items in brief instead of writing words like "Offered", "Complied with" etc.

1. Bidders need to ensure compliance to all the eligibility criteria points.

2. Purchase orders without relevant organization confirmation through a credential letter will not be considered as credentials.

3. Scheduled commercial Banks do not include Regional Rural Banks and Cooperative Banks.

Annexure E: Technical Evaluation

The bidder should meet the technical requirements as mentioned in the table below. The Bank will scrutinize the offers to determine their completeness (including signatures from the relevant personnel), errors, omissions in the technical & commercial offers of respective bidders. The Bank plans to, at its sole discretion, waive any minor non-conformity or any minor deficiency in an offer. The Bank reserves the right for such waivers and the Bank's decision in the matter will be final.

A copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the tender document should also be submitted.

Summary of Technical Evaluation Qualification Criteria

- **Total Technical Score: 300 Marks**

- **Minimum Overall Passing Score: 240 Marks (80%)**

The threshold score for technical qualification would be **240 marks** out of **300 marks** based on the evaluation method given below:

Techno-functional Specifications

S. No	Requirement Area	Requirement Description	Compliance/Remarks	Marks
A	End Point Protection + EDR + Sandbox			
1	Product Requirements	The solution should also offer layered security that helps to catch file less attacks at multiple points in the attack chain. The proposed solution must be on-premises including all required features and components. Single unified agent is mandatory for Anti-Virus, Anti-Malware, Antispyware, File Reputation, Exploit Prevention, Command and Control (C&C) protection, Zero-day Vulnerability Protection, Device Control, Ransomware Protection, Desktop Firewall & Host Intrusion Prevention, Browser IPS, Application Control or File discovery, Active Directory Defence, Active Directory Breach Assessment, Adaptive Security, Threat Intelligence API, Isolation. It is desired and preferred to have other endpoint security solution i.e. EDR/XDR/ATP on a single agent.	Yes/No	2
2	Update Distribution	The proposed solution client shall be loaded on the endpoints and the server shall distribute the updates to the client preferably through Group based distribution or group update provider.	Yes/No	1

3	Central Management	The proposed solution shall provide a Central Management dashboard to manage the entire solution. Solution must provide central management functions in terms of logs, threat intelligence, status of managed products/devices. Central management should work as centralized threat sharing/management server with the managed clients. Solution should be able to provide a central view of threat detections for managed devices. Solution should be able to generate downloadable reports from existing and customizable templates.	Yes/No	**2**
4	Deployment	The proposed solution should be deployed in centralized architecture to manage policies and should be controlled centrally.	Yes/No	**1**
5	Client Platforms Supported	The proposed solution should support the following Operating Systems Platforms- Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025 or later till the time these OS's are not EoL from MS and another OS like Red Hat Enterprise Linux (6,7,8, 9), Oracle, Linux (6,7,8, 9), etc.	Yes/No	**1**

6	Protection Features	The proposed solution should have the following protection mechanism: 1. Anti-Virus 2. Anti-Malware 3. Antispyware 4. File Reputation 5. Exploit Prevention (host firewall, exploit protection) 6. Command and Control (C&C) protection. 7. Zero-day Vulnerability Protection 8. Device Control 9. Ransomware Protection 10. Desktop Firewall & Host Intrusion Prevention 11. Browser IPS 12. Application Control or File discovery 13. Machine Learning-driven Exploit 14. Network Integrity, Wi-Fi Reputation, and Smart VPN 15. Active Directory Defence 16. Active Directory Breach Assessment 17. Adaptive Security 18. Threat Intelligence API 19. Isolation 20. Mobile Threat Protection/Defence 21. File Integrity Monitoring	Yes/No	**2**

7	Installation Method	The proposed solution shall provide following installation methods: 1. EXE/MSI Package based installer 2. Web based installation 3. Login script-based installation 4. Remote installation 5. Through SCCM All the client components should be installed using the single client package	Yes/No	1
8	Uninstallation Protection	The proposed solution should prevent normal host user from uninstalling the endpoint security client	Yes/No	1
9	Unmanaged Endpoint Detection	The proposed solution shall provide detection of endpoints that do not have the agent installed	Yes/No	1
10	Policy	Policy should effect immediately on Realtime/near real time basis on the endpoints	Yes/No	1
B	**Malware Protection**			
1	Anti-Malware	The proposed solution must protect against all kinds of viruses, Trojans and worms including but not limited to: boot sector, master boot sector, memory resident, macro, stealth and polymorphism etc.; and any other forms of exploits.	Yes/No	1
2	Anti-Malware	The proposed solution shall also protect against certain non-virus threats, such as Spyware, adware, dialers, joke programs, remote access and hacking tools, which can be used with malicious intent	Yes/No	1

3	Anti-Malware	The proposed solution should be able to do full scan of files / folders with a choice of specifying directories and file extensions not to be scanned	Yes/No	1
4	Anti-Malware	The proposed solution should provide performance control while scanning files/folders/Hard disk	Yes/No	1
5	Anti-Malware	The proposed solution shall be able to scan only those file types which are potential virus carriers (based on true file type)	Yes/No	1
6	Anti-Malware	The proposed solution should provide high fidelity pre-execution and run-time machine learning to detect emerging unknown security threats, which does not have any signatures	Yes/No	1
7	Anti-Malware	The proposed solution should provide protection against the packer detections (when they unpack) which hides in memory	Yes/No	1
8	Anti-Malware	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser	Yes/No	1
9	Anti-Malware	The proposed solution shall inspect applications, as well as the applications' sub-components (DLLs) as they are executed	Yes/No	1
10	Anti-Malware	The proposed solution shall have the ability to detect applications, which attempt to propagate themselves over the network	Yes/No	1

11	Damage Clean up	The proposed solution on detection of a malware infection, should allow removal of traces of malware from the system by cleaning up the following automatically or via remote remediation console from centralized Management console: a) Detected malicious file b) Affected registry entries c) any new files dropped by malware d) windows services created by malware e) any other system settings affected by malware.	Yes/No	**2**
12	Ransomware Protection	The proposed solution shall protect documents critical files and folders and have options to configure custom file formats and folders from any modifications or encryption.	Yes/No	**1**
13	Protection Against File Less Attacks	The proposed solution shall protect against file less malware and shall utilize behavioural techniques to detect malware based on the behaviour of the file	Yes/No	**1**
14	Tamper Protection	The proposed solution should have tamper protection against malware that attempt to disable security measures	Yes/No	**1**
15	Offline Event Collection	The proposed solution should store event data at endpoint client while it is disconnected from the corporate network and forwards it on reconnection	Yes/No	**1**
16	Botnet Protection	The proposed solution shall provide detection and blocking of Command and control (C&C) traffic and prevent access of malicious and dangerous websites	Yes/No	**1**

17	Enforcement Actions	The proposed solution must provide application of enforcement actions based on malicious file types such as Delete, Block, Quarantine	Yes/No	1
18	Zero Day Malware Detection	The proposed solution shall provide submission of suspicious files to a sandbox / threat- analysis solution for virtual execution / Root-Cause analysis. The sandbox / threat - analysis solution shall provide execution / RCA result for the suspicious file	Yes/No	1
19	Zero Day Malware Detection	The proposed solution shall provide on-premise sandboxing capabilities integration with EDR Appliance.	Yes/No	1
C	**Detection Features**			
1	Start-up Protection	The proposed solution shall protect from malware in memory and boot sector on system start-up	Yes/No	1
2	Real time Protection	The proposed solution shall provide real time protection against malware	Yes/No	1
3	Exclusion List	The proposed solution shall be able to add files, folders or extensions to an exclude list from detection	Yes/No	1
4	Compressed Files	The proposed solution shall protect from malware in compressed file formats like ZIP, RAR etc.	Yes/No	1
D	**Intrusion Prevention System**			

1	Vulnerability Protection	The proposed solution shall protect the endpoint against the exploitation of vulnerabilities in operating system with other applications and should have options to add custom applications.	Yes/No	1
2	Protection Against Illegitimate Traffic	The proposed solution should detect suspicious network traffic. It shall allow blocking of all traffic from the originating endpoint	Yes/No	1
3	Firewall	The proposed solution must provide the flexibility to create firewall rules to filter connections.	Yes/No	1
E	**Application Control/Application whitelisting**			
1	Policy Management	The proposed solution provides a capable allow or deny policy that is able to manage known and unknown applications, file types, and executables	Yes/No	1

2	Policy Rules	a. The proposed solution should allow application whitelisting and blacklisting on basis of application path, regular expression, reputation score and certificate. b. The proposed app control solution should provide monitoring and prevention mode for executing unwanted applications. c. The proposed solution should allow specifying trusted updater to modify device or client application during patch and application updates. d. The solution should provide policy enforcement and allows users to override application Control detections of applications that are not on the allow list or the block list. e. The solution should provide whitelist or blacklist exception using file hash	Yes/No	**2**
3	Reputation Score	The proposed solution is able to provide a reliable file reputation source and global usage details to allow cross checking of known good files. This source must be constantly kept up- to-date with the latest known good file listing	Yes/No	**1**
F	**Device Control**			
1	Device Control	The proposed solution shall have the capability to control usage of external devices including storage devices, Non-storage devices etc. on the endpoint	Yes/No	**1**

2	Blocking of External Devices	The proposed solution should potentially block the endpoint system from loading physical devices on USB bus such as removable storage devices, Bluetooth, Wi-Fi network cards etc.	Yes/No	1
3	Control of Storage Devices	The proposed solution shall provide management of storage devices and allow restrictions on their usage to Monitor, Block or make the device Read-Only along with the option of providing exceptions	Yes/No	1
4	Authorized USB Access & Device Registration	The proposed solution shall allow usage of authorized USB devices by users and blocking of unauthorized USB devices. The solution shall allow exclusion of authorized USB devices by using their vendor ID, product ID or serial number	Yes/No	1
5	Device Control Log	The proposed solution shall provide logs of the device control feature to detect attempts of connecting unauthorized devices	Yes/No	1
G	**Security Definition Updates**			
1	Threat Intelligence and Signature Updates	The proposed solution OEM should have a 24/7 security service update and should support real time updates of the system on release	Yes/No	1
2	Definition / Signature Update Mechanism	The proposed solution shall have an updating mechanism using local update server	Yes/No	1
3	Incremental Updates	The proposed solution shall allow for incremental update of definitions	Yes/No	1

4	Roaming Clients	The proposed solution shall provide a mechanism for updates of roaming devices or clients which are connected to Internet	Yes/No	1
H	**Management and Reporting**			
1	Dashboard	The proposed solution should provide a management dashboard to view the status of endpoints across the enterprise locations/geographies and a central incident response to work on EDR features like detection models, threat hunting and response actions etc. The proposed End-point Protection solution should have possibly real-time dashboard views about the threat activities at the end-point	Yes/No	1
2	Dashboard Features	The proposed solution shall offer enterprise-wide visibility over the status of all the deployed components. The dashboard shall provide a summarized view to analyse top threats & summary of malware traffic or any other threats	Yes/No	1
3	Central Policy Deployment	The proposed solution shall offer creation of granular policies based on flexible attributes which can be deployed with consistent policy enforcement across distributed environments and multiple components from one management platform	Yes/No	1
4	Hierarchical Policies	The proposed solution shall provide hierarchical grouping of machines and policy deployment	Yes/No	1

5	Central Update Repository	The proposed solution shall offer a central repository of the updates that can be distributed to the managed components	Yes/No	1
6	Log Retention	The proposed solution should have minimum log retention period of upto 90 days	Yes/No	1
7	Log Management	The proposed solution shall be able to receive logs from the managed components and endpoints and store them centrally	Yes/No	1
8	Log Forwarding & SIEM Integration	The proposed solution shall collect the events occurring on endpoints. The solution shall also provide the functionality to forward of these events to the SIEM.	Yes/No	1
9	User Alerting	The proposed solution shall provide alerts to users in case of any security incident along with a course of action, in case of any failure to clean	Yes/No	1
10	Administrator Notifications	The proposed solution must provide notifications for important events.	Yes/No	1
11	Role Based Administration	The proposed solution shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges for different components	Yes/No	1
12	Reports	The proposed solution should be capable of providing detailed reports containing data from all the deployed components	Yes/No	1
13	Export of Reports	The proposed solution should allow exporting of reports in readable/presentable format.	Yes/No	1
I	**Endpoint Detection & Response (EDR)**			

1	Impact Assessment	The proposed solution should provide context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls	Yes/No	1
2	Impact Assessment	The proposed solution should be able to perform threat sweep based on the threat feeds received from the integrated sandbox solution as mentioned below 1. IP Address 2. Files 3. URLs 4. Domain	Yes/No	1
3	Root Cause Analysis	The proposed solution should be able to create multi-stage detailed kill-chain for performing the root cause analysis of an incident. Kill chain also provide reputation of the files from the global threat intelligence as well	Yes/No	1
4	Point in time Assessment	The proposed solution should provide option to sweep and assess the current (point in time/Live) state of the devices. 1. Scan disk Files. 2. Scan in memory process 3. Search registry	Yes/No	1

5	Response Action	The proposed solution to provide the advance response capabilities as mentioned below 1. Kill process 2. Isolate device 3. Block process	Yes/No	**1**
6	IOC Ingestion and Blocking	The proposed solution shall allow ingestion of IOCs (Indicators of compromise) like domains, file-hashes and shall also allow blocking of the files/file-hashes/domains/URLs identified by the IOCs	Yes/No	**1**
7	Other Features	The EDR solution should show that, it could contain a threat by Blacklisting, Cleaning, Deleting any event, file, or incident	Yes/No	**1**
8	Other Features	The Solution should review the dashboard to show a comprehensive view of all events occurring in installed modules. Provide key views to incidents that require investigation, as well as all events that are known to have occurred in the environment.	Yes/No	**1**
9	Other Features	The solution Incidents creation should reviewed and filtered by priority and date range.	Yes/No	**1**
10	Other Features	The solution should be able to integrate with the SIEM for event recording from EDR.	Yes/No	**1**
11	Other Features	The solution should have ability to leverage MITRE ATT&CK Framework integration within events\incidents (ID, Tactics, Technique)	Yes/No	**1**

12	Other Features	The solution should have ability to directly connect to the Endpoint for follow up investigation and triage (Live Response)	Yes/No	1
13	Other Features	The solution should support ad-hoc breach assessment report that's provides guidance to reduce domain controller attacks with details on vulnerabilities, misconfigurations, and possible backdoors within the AD.	Yes/No	1
K	**Sandbox Appliance**			
1	Deployment	To be deployed at Data Centre and DR Centre.	Yes/No	1
2	Form Factor	Rack mountable purpose-built dedicated hardware appliance-based solution	Yes/No	1
3	Integration	The proposed appliance should integrate with proposed EPP+EDR solution.	Yes/No	1
4	Virtual Execution	The solution must utilize purpose built On-premise appliance to identify malware, including zero-day exploits, polymorphic/ metamorphic payloads and obfuscated java-scripts.	Yes/No	1

5	File Formats Supported for Inspection	The solution should have the ability to analyse and detect malware in common file formats including (but not limited to) the following types: 1. Compressed archives – Zip, Rar 2. Common Text document Formats: MS Word formats (doc, docx), pdf 3. Common Spreadsheet formats: MS Excel formats (xls, xlsx) 4. Presentation formats: MS PowerPoint formats (ppt, pptx). 5. Common Executable Formats: exe, dll, jar All software licenses required for analysing above file types are in the scope of bidder.	Yes/No	**1**
6	Resistance to Evasion	The virtual execution environment must not be detectable by malware in order to evade detection.	Yes/No	**1**
7	Full Malware Lifecycle Analysis	The malware analysis solution should cover the entire attack lifecycle: execution path, file activity. Registry activity, network activity (call back destinations and subsequent download attempts) and should provide an environment to have in-depth analysis of the malicious file/code within the deployed premise.	Yes/No	**1**
8	Instances Supported	The single appliance should be able to support upto multiple virtual instances in a single appliance.	Yes/No	**1**
9	Operating Systems	The solution should be able to support following operating systems Win 10, Win 11, Win Server 2016, 2019, 2022, 2025 or later	Yes/No	**1**

10	Dashboard	The solution should have a management dashboard to view real time threat visibility and attack characteristics.	Yes/No	**1**
11	Captured Threat data	The solution should store the files submitted to the sandbox for further analysis.	Yes/No	**1**
12	Event Notification	Notifications should be sent to administrators in case of warnings & critical events.	Yes/No	**1**
13	Notification Methods	Multiple notification methods shall be supported like email and SNMP traps etc.	Yes/No	**1**
14	Web Based Management	Web based Management shall be available for local administration.	Yes/No	**1**
L	**Anti-Malware Protection**			
1	Malware Protection	The solution must protect against all kinds of viruses, Trojans and worms including but not limited to: boot sector, master boot sector, memory resident, macro, stealth and polymorphism etc.; and any other forms of exploits	Yes/No	**1**
2	Malware Protection	The solution shall also protect against certain non-virus threats, such as Spyware, adware, dialers, joke programs, remote Access and hacking tools, which can be used with malicious intent	Yes/No	**1**
3	Application Inspection	Solution shall inspect applications, as well as the applications' sub-components (DLLs) as they are executed	Yes/No	**1**
4	Application Inspection	Solution shall have the ability to detect applications that attempt to spread themselves over the network	Yes/No	**1**

5	Enforcement Actions	The solution must provide application of customized enforcement actions based on malicious file types such as Delete, Block, Quarantine	Yes/No	1
6	Damage Clean-up	On detection of a malware infection, the solution should allow removal of traces of malware from the system by cleaning up the following automatically or via remote remediation from a centralized management console: a) Detected malicious file b) Affected registry entries c) Any new files dropped by malware d) Windows services created by malware e) Any other system settings affected by malware	Yes/No	2
7	Ransomware Protection	The solution shall protect documents against unauthorized encryption or modification	Yes/No	1
8	File less Attacks	The solution shall protect against file less malware	Yes/No	1
M	**Detection Features**			
1	Start-up Protection	The solution shall protect from malware in memory and boot sector on system start-up	Yes/No	1
2	Real Time Protection	The solution shall provide real time protection against malware	Yes/No	1
3	Exclusion List	The solution should be able to add files, folders or extensions to an exclude list from detection	Yes/No	1
4	Compressed Files	The solution shall protect from malware in compressed file formats	Yes/No	1

5	Web Reputation	The solution shall detect access of malicious and dangerous websites	Yes/No	1
N	**Advanced Malware Protection for Windows Systems**			
1	Machine Learning	The solution shall utilize machine learning on Windows systems to detect malware, which do not have any signatures	Yes/No	1
2	Behavioural Monitoring	The solution shall utilize behavioural techniques on Windows systems to detect malware based on the behaviour of the file	Yes/No	1
3	Zero Day Malware Detection	The solution shall provide submission of suspicious files to a sandbox / threat-analysis solution for virtual execution / Root-Cause analysis. The sandbox / threat -analysis solution shall provide execution / RCA result for the suspicious file	Yes/No	1
4	Zero Day Malware Detection	The solution shall provide on-premise sandboxing capabilities	Yes/No	1
5	Machine Learning	The solution shall utilize machine learning on Windows systems to detect malware, which do not have any signatures	Yes/No	1
O	**Firewall**			
1	Rules	Firewall rules should Filter traffic based on source and destination IP address, port, MAC address, etc.	Yes/No	1
2	Reconnaissance	Solution should detect reconnaissance activities such as port scans and Solution should be capable of blocking and detecting Ipv4/IPv6 attacks	Yes/No	1
P	**Host Intrusion Prevention System**			

1	Vulnerability Protection	The solution shall protect against known and un-known vulnerabilities and provide complete security against zero-day vulnerabilities without any new signatures	Yes/No	1
2	Rules Enforcement	Should provide enforcement of HIPS rules against known and unknown vulnerabilities for OS and Applications. Besides, solution should support auto sandboxing feature to add custom applications like core banking etc from any vulnerabilities	Yes/No	1
3	Illegitimate Traffic	The solution should detect suspicious network traffic. It shall allow blocking of all traffic from the originating servers	Yes/No	1
Q	**Application Control**			
1	Application Control	The solution shall have the capability of restrict usage of unauthorized applications and enable blacklist/whitelist of applications on the server	Yes/No	1
R	**Integrity Monitoring**			
1	Integrity Monitoring	The solution shall provide real time integrity monitoring of critical operating system and application elements such as directories, files, registry keys and values to detect and report suspicious activity such as modifications	Yes/No	1
2	Rules Enforcement	The solution shall provide options to enforce the integrity monitoring rules which are applicable for the servers	Yes/No	1

3	Threat Intelligence and Signature Updates	The OEM should have a 24/7 security service update and should support real time signature update of the system as soon as updates are released	Yes/No	1
4	Security Update Mechanism	The solution shall have an updating mechanism using local update server	Yes/No	1
S	**Management**			
1	Unified Central Dashboard	The solution should provide a single unified management dashboard to view the status of installed agents	Yes/No	1
2	Dashboard Features	The solution shall offer enterprise-wide visibility over the status of all the deployed components from a central dashboard. The dashboard shall provide a summarized view to analyze top threats & summary of malware traffic or any other threats	Yes/No	1
3	Central Policy Deployment	The solution shall offer creation of granular policies based on flexible attributes which can be deployed with consistent policy enforcement across distributed environments and multiple components from one management platform	Yes/No	1
4	Central Update Repository	The solution shall offer a central repository of the updates that can be distributed to the managed components	Yes/No	1
5	Log Management	The solution shall be able to receive logs from the managed servers and store them centrally	Yes/No	1

6	Log forwarding & SIEM Integration	The solution shall collect the events occurring on servers. The solution shall also provide the functionality to forward of these events to the SIEM	Yes/No	1
7	User Alerting	The solution shall provide alerts to users in case of any security incident	Yes/No	1
8	Administrator Notifications	The solution must provide notifications for important events. The notifications must be sent through email or SNMP traps	Yes/No	1
9	Role Based Administration	The solution shall support multiple administrator/full access roles accounts. Each administrator account shall be configurable with the desired level of management privileges for different components	Yes/No	1
10	Audit Trail	Solution should provide logging of administrative activities performed by the administrators	Yes/No	1
11	Reporting	The proposed solution should be capable of providing detailed reports containing data from all the deployed components	Yes/No	1
12	Export of Reports	Exporting of reports to PDF or text format shall be available	Yes/No	1
T	**Licensing**			
1	Licensing	The solution shall be supplied with all necessary licenses and subscriptions including Antimalware, Host IPS, Application Control, File Integrity monitoring, Application sandbox, Central management etc.	Yes/No	1
U	**XDR (Extended Detection and Response)**			

1	The solution should detect malicious activity within customer environment, cross-infection and compromised hosts.	Yes/No	1
2	The solution threat analytics should have Built-in threat expertise and global threat intelligence to detect investigate and respond	Yes/No	1
3	The solution threat analytics should combine threat and detection data from the environment with global threat intelligence for richer, more meaningful alerts	Yes/No	1
4	The solution should be able to identify the high priority at-risk vulnerabilities for Microsoft supported Windows Operating Systems and MS Office in enterprise using global activity data, CVE information, and local detection activity from the endpoints to produce customized vulnerability detection scores for each endpoint. The supported environment for this feature	Yes/No	1
5	The solution should also be able to identify the exploits attempts against the identified high priority vulnerabilities	Yes/No	1
6	The solution threat analytics should provide more context leading to faster detection and higher fidelity alerts while correlating telemetry feeds from the EDR	Yes/No	1
7	The solution threat analytics should use Optimal AI and analytics providing with a deeper understanding of data collected from sensors like EDR	Yes/No	1
8	The solution should store data in central repository which should be hosted within India only	Yes/No	1
9	The solution should support search based on Structured Threat Information Expression and allow analysts to do standard or in combinations searches from the pre-defined attributes which span across endpoints	Yes/No	1
10	The solution repository should have Activity data as well as Detection data (which should be mapped to MITRE TTPs framework)	Yes/No	1

11	The solution should allow for search irrespective of the machine being online or offline	Yes/No	1
12	The solution threat analytics can do multi-layer correlation so that activity that may not seem suspicious on its own suddenly becomes a high-priority alert, allowing to contain its impact faster.	Yes/No	1
13	The solution should also assist customer to quickly create the attack visualization graph, which also shows the impact scope, MITRE TTPs mapping with the activity data and also help analyst to take the remediation steps from the same graph	Yes/No	1
14	The solution should be ONE source of prioritized alerts based on one expert alert schema to interpret data in a standard and meaningful way	Yes/No	1
15	The solution threat analytics with AI and Data should negate the need for doing multiple investigations and should provide a complete triage of all the assets involved in that attack.	Yes/No	1
16	The proposed XDR solution should be on-premises with all required components. Cloud solution shall not be acceptable	Yes/No	1
17	The solution should be in high availability mode at DC and DR	Yes/No	1
18	The solution should provide a Service Level Objective (SLO) to the customer	Yes/No	1
19	The solution should be able to support Multi-factor Authentication (MFA)	Yes/No	1
20	The solution should be able to monitor and investigate endpoints regardless of their location—on premises or remote,	Yes/No	1

21	The solution should be able to provide the minimum below dashboard for threat and assets visibility 1. MITRE ATT&CK Mapping 2. At-Risk Users & Devices 3. Top Risky Cloud Apps 4. Top Endpoint with Detections 5. Company Risk Index	Yes/No	**1**
22	The solution to provide the threat prioritization via the attack visualization graph along with attack severity and cumulative score for that threat investigation chain 1. Solution to easily identify the point of entry of an attack 2. Ability to identify all the hosts that are infected of the same threat 3. Ability to display in a single view the entire threat attack lifecycle	Yes/No	**1**
23	The solution should allow to analyst to take the below remediation actions 1. Isolate Endpoint (Windows, Mac) 2. Remote Shell (Windows, Mac) 3. Terminate Process (Windows, Mac) 4. Collect File (Windows, Mac) 5. Run Remote Custom Script (Windows, Mac) 6. Memory Dump (Windows, Mac)	Yes/No	**1**
24	The solution should visualize root cause analysis (RCA) report and explanation for suspicious objects	Yes/No	**1**
25	The solution should use a blend of advanced threat protection techniques to eliminate security gaps across any user activity and any endpoint, that constantly learns, adapts, and automatically shares threat intelligence across your environment	Yes/No	**1**

26	The solution should have the capability to automatically detect and respond to the ever-growing variety of threats, including file less attacks and ransomware	Yes/No	**1**
27	The solution should provide central visibility and control to be managed through a single console	Yes/No	**1**
28	The solution should combine machine learning along with pattern-based intelligence with other advanced detection techniques for the broadest protection against multiple threats sources may it be known or unknown.	Yes/No	**1**
29	The solution should have the capability to progressively filter out threats using the most efficient tactics and techniques to minimize the attack surface.	Yes/No	**1**
30	The solution should provide noise cancellation techniques such as census and whitelist checking to drastically reduce false positives at each layer.	Yes/No	**1**
31	The solution should have the ability to clean infected files, perform rollback and even recover lost files if necessary	Yes/No	**1**
32	The solution should be able to provide a good consumer experience by having minimal impact to performance through the use of right detection technique at the right time and low management costs	Yes/No	**1**
33	The solution should be able to provide off-premises compliance and protection which enables employees to work outside the corporate network and still be covered by the company security solution.	Yes/No	**1**
34	The solution should provide a flexible choices of security agent deployment. It must be able to support mass deployment through the network and remote offices. It must also support uninstallation of 3rd party security agents.	Yes/No	**1**

35	The solution should support automatic sharing of threat intelligence across security layers enabling protection from emerging threats across the whole organization	Yes/No	**1**
36	The solution should support Open Standard – STIX/TAXII for threat intelligence sharing	Yes/No	**1**
37	The solution should have a centralized security management console to ensure consistent security management and complete visibility and reporting across multiple layers of interconnected security and eliminate redundant and repetitive tasks in security administration.	Yes/No	**1**
38	The solution should have options of creating custom dashboard, and able to create users with different user roles for managing the solution.	Yes/No	**1**
39	The solution should be able to integrate with Active Directory, two factor authentications etc.	Yes/No	**1**
40	The solution should provide complete threat visibility i.e. End-to-end details of threats such as compromised IT asset, malware, IOCs / IOAs, threat actor, tools, tactics and procedures.	Yes/No	**1**
41	The solution should provide out-of-the-box integration with one or more threat intelligence feed to identity potential threats in the Bank's environment.	Yes/No	**1**
42	The solution should integrate, correlate, and contextualizes data and incidents from bank's security tools across all control points, including endpoint, network, web, email, DLP etc.	Yes/No	**1**
43	The solution should response/share IOCs/Threats details to the Bank's implemented various security solutions.	Yes/No	**1**
44	The solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network, and Active Directory to their repository for correlation, threat detection, threat hunting and response	Yes/No	**1**

45	The solution should have advanced incident response capabilities across different channels viz. endpoint, server, network, and cloud in both manual and automated manner.	Yes/No	**1**
46	The solution should allow search / sweeping of Indicators of Compromise (IOCs) / Indicators of Attack (IOAs) in the Bank's environment to support faster threat hunting and remediation.	Yes/No	**1**
47	The proposed solution should integrate with Bank's SIEM tool for automatic raising of incidents as and when triggered in the solution.	Yes/No	**1**
48	The Solution should enrich all data drawn from managed devices with authoritative threat intelligence	Yes/No	**1**
49	The solution should have native control points owned by OEM and shouldn't be a hybrid XDR, where control points are partially owned and partially achieved via integrations with 3rd party security solutions	Yes/No	**1**
50	The solution should apply root cause analysis process & workflow to data from multiple control points. It should also provide additional data that provides context and speeds investigation	Yes/No	**1**
51	The solution should unify and analyze aspects of an attack to be seen from a single console. It should generate prioritized alerts via context from multiple control points	Yes/No	**1**
52	The solution should provide insight about how to prioritize response to multiple incidents and enable multiple teams to apply collective expertise to an attack	Yes/No	**1**
53	The solution should detect data exfiltration by detecting anomalous user login & file download activity, scanning downloaded content policies, correlating sensitive data access with suspicious endpoint activity and identifying scope of data access in case of breach	Yes/No	**1**

54	The solution should be able to automate the response to build the policy required at various security solutions on response shared to protect the environment	Yes/No	1
55	The solution should have an option of various alerting methods such as email/ SMS/ SIEM integration	Yes/No	1

Technical Evaluation Qualification Criteria

S. No	Criteria	Evaluation Parameters	Max Marks
1	ISO 9001 & ISO27001 Certifications of Bidder	2.5 marks for each certification	5
2	OEM Capability & Experience in implementation of proposed solution in Commercial Banks/BFSI during last 5 years	5 marks for each Implementation	20
2	Bidder's Capability & Experience in implementation of proposed solution in Commercial Banks/BFSI during last 5 years	For each Implementation 5 marks	25
3	Techno-functional Specification	Marks defined in table above	190
4	Technical Presentation / Product Demo	Committee Scoring	60

Total Marks	**300 Marks**

We hereby confirm that our proposed Solution meet all the specifications as mentioned above and have submitted the supporting documents against each point claimed.

Signature and Seal of Company

Date:

Annexure F: Commercial Bid Format

1. These details should be on the letter head of the bidder and each & every page should be signed by an authorized signatory with name and seal of the company.

2. Please be guided by RFP terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.

3. Do not change structure of format nor add any extra items.

4. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.

The Commercial Bid shall be submitted in the following format:

Part A

S. No.	Item Details	Qty (X)	Rate Per Unit (Y)	Cost for 3 years (Rs) Z = X*Y*3	Amount in Words
1	Endpoint Detection and Response (EDR) Solution with Advanced XDR Capabilities – Licensed Latest Version with support	11500			
2	L2 Onsite Support at Banks DC location	1			
Part (A) Total					

***Taxes shall be extra as applicable.**

Part B

S. No.	Item Details	Total Cost in Rs	Amount in Words
1	One-time implementation cost for the project (If applicable)		
2	Appliance Cost (if applicable) across DC/DR with 3 years AMC		

3	Database License Cost (if non-oracle) across DC/DR with 3 years AMC		
Part (B) Total			

***Taxes shall be extra as applicable.**

*** In case, the solution uses oracle as database, same shall be provided by the bank and the bidder(s) shall not require to factor it in commercials.**

Grand Total

Item Details	Amount in Rupees	Amount in Words
Part (A) Total		
Part (B) Total		
Grand Total= Part (A) Total + Part (B) Total		

***Taxes shall be extra as applicable.**

Payment Terms:

a. The payment against the subscription of licenses shall be post activation of licenses and shall be paid yearly in advance.

b. The payment against one-time implementation cost shall paid post rendering of services.

c. The payment against the L2 support shall be paid, half-Yearly post rendering of services.

d. In case of any additional license requirement during the contract period, the Bidder shall provide the additional licenses at the same rate as finalized in purchase order. The price of additional licenses shall remain applicable from the date of activation of such licenses till the end of the contract period.

e. The P.O. shall be governed by the terms of agreement (Master Sales and Services agreement) to be executed between J&K Bank & successful bidder within 45 days from date of Issuance of this PO.

f. Until the signing of formal contract, the relation shall be governed by the terms of RFP and all the terms as stipulated in RFP shall apply.

g. Prices mentioned above are exclusive of taxes and taxes shall be extra as and if applicable.

h. The company shall submit PBG of 5% of the total project cost as a Performance Guarantee for the period of contract.

i. Payments shall be released on delivery / implementation and followed up by activation of licenses subject to clause (d) and post confirmation from the Bank.

j. The contract shall remain valid for a period of three year.

k. License activation will start from the date of Go-Live (Not from the issuance of purchase order or without confirmation of the bank).

Signature with Seal **Date:**

Name:

Designation:

Annexure G: Bank Guarantee Format

Dated:_____

Bank:_____

To

Jammu & Kashmir Bank M.A. Road, Srinagar,

190 001 J&K.

WHEREAS..... (Company Name) and having its Registered Office at..... India (hereinafter referred to as "the Bidder") proposes to respond to RFP No ....., dated ..... of Jammu and Kashmir Bank Ltd for selection of vendor for ..... (Herein after called the "RFP") AND

WHEREAS, in terms of the conditions as stipulated in the RFP, the bidder is required to furnish a Bank Guarantee in lieu of the Earnest Money Deposit (EMD), issued by a scheduled commercial bank in India in your favour to secure the order under Schedule 1 of the RFP in accordance with the RFP Document (which guarantee is hereinafter called as "BANK GUARANTEE") AND WHEREAS the bidder has approached us, ... for providing the BANK GUARANTEE.

AND WHEREAS at the request of the bidder and in consideration of the proposed RFP to you, We ,.....having Branch Office/Unit amongst others at....., India and registered office/Headquarter at.....have agreed to issue the BANK GUARANTEE.

THEREFORE, We, ..., through our local office at..... India furnish you the Bank GUARANTEE in manner hereinafter contained and agree with you as follows:

1. We....., undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from you and undertake to indemnify you and keep you indemnified from time to time to the extent of

Rs.....(Rupees .....only) an amount equivalent to the EMD against any loss or damage caused to or suffered by or that may be caused to or suffered by you on account of any breach or breaches on the part of the bidder of any of the terms and conditions contained in the RFP and in the event of the bidder commits default or defaults in carrying out any of the work or discharging any obligation in relation thereto under the RFP or otherwise in the observance and performance of any of the terms and conditions relating thereto in accordance with the true intent and meaning thereof, we shall forthwith on demand pay to you such sum or sums not exceeding the sum of Rs.....(Rupees..... only) as may be claimed by you on account of breach on the part of the bidder of their obligations in terms of the RFP. Any such demand made on the Bank shall be conclusive as regards amount due and payable by the Bank under this guarantee.

2. Notwithstanding anything to the contrary contained herein or elsewhere, we agree that your decision as to whether the bidder has committed any such default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you to establish your claim or claims under Bank Guarantee but will pay the same forthwith on your demand without any protest or demur.

3. This Bank Guarantee shall continue and hold good until it is released by you on the application by the bidder after expiry of the relative guarantee period of the RFP and after the bidder had discharged all his obligations under the RFP and produced a certificate of due completion of work under the said RFP and submitted a " No Demand Certificate " provided always that the guarantee shall in no event remain in force after the day of .....without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.

4. Should it be necessary to extend Bank Guarantee on account of any reason whatsoever, we undertake to extend the period of Bank Guarantee on your request under intimation to the SI/OEM till such time as may be required by you. Your decision in this respect shall be final and binding on us.

5. You will have the fullest liberty without affecting Bank Guarantee from time to time to vary any of the terms and conditions of the RFP or extend the time of performance of the RFP or to postpone any time or from time to time any of your rights or powers against the bidder and either to enforce or forbear to enforce any of the terms and conditions of the said RFP and we shall not be released from our liability under Bank Guarantee by exercise of your liberty with reference to matters aforesaid or by reason of any time being given to the bidder or any other forbearance, act or omission on your part of or any indulgence by you to the bidder or by any variation or modification of the RFP or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of so releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs.....(Rupees.....only) as aforesaid or extend the period of the guarantee beyond the said day of ..... unless expressly agreed to by us in writing.

6. The Bank Guarantee shall not in any way be affected by your taking or giving up any securities from the bidder or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency or death as the case may be of the bidder

7. In order to give full effect to the guarantee herein contained, you shall be entitled to act as if we were your principal debtors in respect of all your claims against the bidder hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of Bank Guarantee.

8. Subject to the maximum limit of our liability as aforesaid, Bank Guarantee will cover all your claim or claims against the bidder from time to time arising out of or in relation to the said RFP and in respect of which your claim in writing is lodged on us before expiry of Bank Guarantee.

9. Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax or registered post to our local address as aforesaid and if sent accordingly it shall be deemed to have been given when the same has been posted.

10. The Bank Guarantee and the powers and provisions herein contained are in addition to and not by way of limitation of or substitution for any other guarantee or guarantees here before given to you by us (whether jointly with others or alone) and that Bank Guarantee is not intended to and shall not revoke or limit such guarantee or guarantees.

11. The Bank Guarantee shall not be affected by any change in the constitution of the bidder or us nor shall it be affected by any change in your constitution or by any amalgamation or absorption thereof or therewith but will ensure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.

12. The Bank Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.

13. We undertake to pay to you any money so demanded notwithstanding any dispute or disputes raised by the bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present being absolute and unequivocal.

14. The Bank Guarantee needs to be submitted in online form also via SFMS Application.

15. Notwithstanding anything contained herein above;
    i. our liability under this Guarantee shall not exceed Rs.....(Rupees.....only) ;

    ii. this Bank Guarantee shall be valid up to and including the date ..... _____and claim period shall be upto _____ ; and

    iii. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before the expiry of the claim period.

16. We have the power to issue this Bank Guarantee in your favour under the Memorandum and Articles of Association of our Bank and the undersigned has full power to execute this Bank Guarantee under the Power of Attorney issued by the Bank.

For and on behalf of BANK

Authorized Signatory

Seal

Address

Annexure H: Performance Bank Guarantee Format

To

The Jammu & Kashmir Bank M.A. Road, Srinagar,

190 001 J&K.

WHEREAS..... (Company Name) registered under the Indian Companies Act 1956 and having its Registered Office at ....., hereinafter referred to as the VENDOR has for taken up for..... ....in terms of the Purchase Order bearing No. ..... Dated ....., hereinafter referred to as the CONTRACT. AND WHEREAS in terms of the Conditions stipulated in the said Contract, the VENDOR is required to furnish, performance Bank Guarantee issued by a Scheduled Commercial Bank in your favor to secure due and satisfactory compliance of the obligations of the VENDOR in accordance with the Contract; THEREFORE, WE, ..., through our local office at ..... Furnish you this Performance Guarantee in the manner hereinafter contained and agree with you as follows:

1. We, ... do hereby undertake to pay the amounts of ₹..... and payable under this Guarantee without any demur, merely on a demand, which has to be served on us before the expiry of this guarantee, time being essence of the contract, from you stating that the amount claimed is due by way of loss or damage caused to or would be caused to or suffered by you by reason of breach by the said vendor of any of the terms and conditions contained in the Contract or by reason of the vendor's failure to perform the said contract. Any such demand made on us within the time stipulated above shall be conclusive as regards the amount due and payable by us under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding..... (Rupees ..... Only).
2. We undertake to pay to you any money so demanded notwithstanding any dispute/s raised by the vendor in any suit or proceeding before any Court or Tribunal relating thereto, our liability under these presents being absolute and unequivocal. The payment so made by us under this

guarantee shall be a valid discharge of our liability for payment there under and the vendor shall have no claim against us for making such payment.

3. We further agree that, if demand, as stated above, is made on us within the stipulated period, the guarantee herein contained shall remain in full force and effect and that it shall continue to be enforceable till all your dues under or by virtue of the said contract have been fully paid and your claims satisfied or discharged or till you certify that the terms and conditions of the said contract have been fully and properly carried out by the said vendor and accordingly discharge this guarantee. Provided, however, serving of a written claim / demand in terms hereof on us for payment under this guarantee on or before the stipulated period, time being the essence of contract, shall be a condition precedent for accrual of our liability / your rights under this guarantee.

4. We further agree with you that you shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder, to vary any of the terms and conditions of the said Contract or to extend time for performance by the said vendor from time to time or to postpone for any time or from time to time any of the powers exercisable by us against the said VENDOR and to forbear or enforce any of the terms and conditions relating to the said Contract and we shall not be relieved from our liability by reason of such variation, or extension being granted to the said Vendor or for any forbearance, act or omission on our part or any indulgence by us to the said vendor or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

5. This Guarantee will not be discharged due to the change in the constitution of our Bank or the Vendor.

6. We further agree and undertake unconditionally without demur and protest to pay you the amount demanded by you in writing irrespective of any dispute or controversy between you and the VENDOR.

7. We lastly undertake not to revoke this guarantee during its currency except with your written Consent. NOTWITHSTANDING anything contained herein above;

(i) Our liability under this Guarantee shall not exceed.....Rupees..... .only);

(ii) This Guarantee shall be valid up to .....; and claim period of this Bank Guarantee shall be ..... year/s after expiry of the validity period i.e., up to.....; and

(iii) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before the expiry of this guarantee.

Dated the..... Day of .....20.....

For.....

BANK Authorized Signatory

Annexure I: Non-disclosure Agreement (NDA)

THIS NON-DISCLOSURE AGREEMENT (the "Agreement") is made and entered into as of (____/____/2026) by and between

_____, a company incorporated under the laws of India, having its registered address at _____ (the "Receiving party/Company") and

"Jammu and Kashmir Bank Ltd, a Banking Company under Indian Companies Act,2013 having corporate and registered office at M. A. Road, Srinagar, J&K, India-190001 represented herein by Authorized Signatory (hereinafter referred as Bank/Disclosing Party which unless the context requires include its successors in interests and permitted assigns). (the "Bank/Disclosing Party").

The Company/Receiving party and Bank/Disclosing Party are hereinafter collectively referred to as parties and individually as a party.

Whereas the parties have entered into contract and for performance of contract, the parties may share/disclose certain proprietary/confidential information to each other. To protect the confidentiality of the confidential information shared/disclosed, the parties hereto have entered into this NDA.

NOW THEREFORE THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. **Purpose** J&K Bank/Disclosing Party has engaged or wishes to engage the Company/Receiving party for undertaking the project vide Purchase Order No: _____(and subsequent POs issued in this regard) and each party may disclose or may come to know during the course of the project certain confidential technical and business information which the disclosing party desires the receiving party to treat as confidential.

2. **Confidential Information** means any information disclosed or acquired by other party during the course of the projects, either directly or indirectly, in writing, orally or by inspection of tangible objects (including without limitation documents, prototypes, samples, technical data, trade secrets, know-how, research, product plans, services, customers, markets, software, inventions, processes, designs, drawings, marketing plans, financial

condition and the Company's plant and equipment), which is designated as "Confidential," "Proprietary" or some similar designation. Information communicated orally shall be considered Confidential Information if such information is confirmed in writing as being Confidential Information within a reasonable time after the initial disclosure. Confidential Information may also include information disclosed to a disclosing party by third parties. Confidential Information shall not, however, include any information which

i. was publicly known and made generally available in the public domain prior to the time of disclosure by the disclosing party;

ii. becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party;

iii. is already in the possession of the receiving party at the time of disclosure by the disclosing part as shown by the receiving party's files and records immediately prior to the time of disclosure;

iv. is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality;

v. is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as shown by documents and other competent evidence in the receiving party's possession; or

vi. Is required by law to be disclosed by the receiving party, provided that the receiving party gives the disclosing party prompt written notice of such requirement prior to such disclosure and assistance in obtaining an order protecting the information from public disclosure.

3. Non-use and non-disclosure. Each party agrees not to use any Confidential Information of the other party for any purpose except to evaluate and engage in discussions concerning a potential business relationship between the parties. Each party agrees not to disclose any Confidential Information of the other party to third parties or to such party's employees, except to those employees of the receiving party who are required to have the information in order to evaluate or engage in discussions concerning the contemplated business relationship. Neither party shall reverse engineer, disassemble, or decompile any prototypes, software or

other tangible objects which embody the other party's Confidential Information and which are provided to the party hereunder.

4. Maintenance of Confidentiality. Each party agrees that it shall take reasonable measures to protect the secrecy of and avoid disclosure and unauthorized use of the Confidential Information of the other party. Each party shall take at least those measures that it takes to protect its own most highly confidential information and shall ensure that its employees who have access to Confidential Information of the other party have signed a non-use and non-disclosures agreement in content similar to the provisions hereof, prior to any disclosure of Confidential Information to such employees. Neither party shall make any copies of the Confidential Information of the other party unless the same are previously approved in writing by the other party. Each party shall reproduce the other party's proprietary rights notices on any such approved copies, in the same manner in which such notices were set forth in or on the original. Each party shall immediately notify the other party in the event of any unauthorized use or disclosure of the Confidential Information.

5. No Obligation. Nothing herein shall obligate either party to proceed with any transaction between them and each party reserves the right, in its sole discretion, to terminate the discussions contemplated by this Agreement concerning the business opportunity. This Agreement does not constitute a joint venture or other such business agreement.

6. No Warranty. All Confidential Information is provided by Bank as "AS IS." Bank/Disclosing Party makes no warranties, expressed, implied or otherwise, regarding its accuracy, completeness or performance.

7. Return of Materials. All documents and other tangible objects containing or representing Confidential Information which have been disclosed by either party to the other party, and all copies thereof which are in the possession of the other party, shall be and remain the property of the disclosing party and shall be promptly returned to the disclosing party upon the disclosing party's written request.

Receiving Party shall immediately return and redeliver to Disclosing Party/ Bank all tangible material embodying the Confidential Information provided hereunder and all notes, summaries, memoranda, , records, excerpts or derivative information deriving there from and all other documents or materials ("Notes") (and all copies of any of the foregoing, including

"copies" that have been converted to computerized media in the form of image, data or word processing files either manually or by image capture) based on or including any Confidential Information, in whatever form of storage or retrieval, upon the earlier of (i) the completion or termination of the dealings between the parties contemplated hereunder; (ii) the termination of the Master Agreement; or (iii) at such time as the Disclosing Party/ Bank may so request.

The receiving party shall destroy /dispose off the confidential information provided by the disclosing party together with its copies upon written request of the disclosing party, as per the directions issued by the disclosing party and such destruction shall be confirmed in writing by receiving party.

8. No License. Nothing in this Agreement is intended to grant any rights to either party under any patent, mask work right or copyright of the other party, nor shall this Agreement grant any party any rights in or to the Confidential Information of the other party except as expressly set forth herein.

9. Term. The Obligations of each receiving party hereunder shall survive even after this agreement except as provided herein above.

10. Adherence. The content of the agreement is subject to adherence audit by J&K Bank. It shall be the responsibility of the Company/Receiving party to fully cooperate and make available the requisite resources/evidences as mandated by J&K Bank Supplier Security policy.

11. Remedies. Each party agrees that any violation or threatened violation of this Agreement may cause irreparable injury to the other party, entitling the other party to seek injunctive relief in addition to all legal remedies.

12. Arbitration, Governing Law & Jurisdiction. In the case of any dispute arising upon or in relation to or in connection with this Agreement between parties, the disputes shall at the first instance be resolved through negotiations. If the dispute cannot be settled amicably within fourteen (14) days from the date on which either Party has served written notice on the other of the dispute then any party can submit the dispute for arbitration under Arbitration and conciliation Act,1996 through sole arbitrator to be appointed mutually by the parties.

The place of Arbitration shall be Srinagar, India and the language of the arbitration proceedings and that of all the documents and communications between the parties shall be English.

The decision of the arbitrator shall be final and binding upon the parties. The expenses of the arbitrator as determined by the arbitrator shall be borne equally.

The parties shall continue to be performing their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration. This agreement shall, in all respects, be governed by, and construed in accordance with the Laws of the UT of J&K read with applicable Laws of India. The Courts in Srinagar India shall have exclusive jurisdiction in relation to this agreement.
All notices or other communication under or in connection with this agreement shall be given in writing and may be sent by personal delivery, or post or courier or facsimile or email. Any such notice or other communication will be deemed to be effective if sent by personal delivery, when delivered, if sent by post, five days after being deposited in the post office and if sent by courier, three days after being deposited with the courier, if sent by facsimile, when sent (on receipt of a confirmation of having been sent to correct facsimile number) and if sent my mail (on receipt of confirmation).

_____ (contact details of Company/Receiving party)

_____ (contact details of Bank/Disclosing Party).

13. Miscellaneous. This Agreement shall bind and intended for the benefit of the parties hereto and their successors and assigns. This document contains the entire Agreement between the parties with respect to the subject matter hereof, and neither party shall have any obligation, express or implied by law, with respect to trade secret or propriety information of the other party except as set forth herein. Any failure to enforce any provision of this Agreement shall not constitute a waiver thereof or of any other provision.

Any provision of this Agreement may be amended or waived if, and only if such amendment or waiver is in writing and signed, in the case of amendment by each Party, or in the case of a waiver, by the party against whom the waiver is to be effective".

The undersigned represent that they have the authority to enter into this Agreement on behalf of the person, entity or corporation listed above their names.

COMPANY NAME	**Bank**
By:_____	By:_____
Name: _____	Name: _____
Title: _____	Title: _____
Address:_____	Address:_____
_____	_____
Company Seal	Company Seal

Annexure J: Undertaking

Bidder has to submit Undertaking on company letter head as per format given below

To

Chief Information Security Officer

Information Security Department.

Corporate Headquarters

The Jammu & Kashmir Bank M.A. Road, Srinagar,

190 001 J&K.

Dear Sir,

Sub: RFP no: _____ for selection of bidder for Endpoint Detection & Response (EDR) Solution with Advanced XDR Capabilities.

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide _____to Bank as mentioned in RFP document in conformity with the said tender documents in accordance with the Commercial bid and made part of this tender.

We understand that the RFP provides generic specifications about all the items and it has not been prepared by keeping in view any specific bidder.

We understand that the RFP floated by the Bank is a confidential document and we shall not disclose, reproduce, transmit or made available it to any other person.

We have read, understood and accepted the terms/ conditions/ rules mentioned in the RFP including the conditions applicable to reverse auction proposed to be followed by the Bank.

Until a formal contract is prepared and executed, this tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us.

We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India and the UT of J&K including Prevention of Corruption Act 1988.

We have never been barred/black-listed by any regulatory / statutory authority in India.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

We hereby undertake that all the components/parts/assembly/software used in the Networking Hardware shall be original new components / parts / assembly / software only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / Parts / Assembly / Software are being used or shall be used.

This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We enclose cost of RFP Rs. 5000/- (Five Thousand Only) and EMD of 24,00,000/- (INR Twenty -Four Lakh Rupees only) in Bank Transfer/Demand Draft/Bank Guarantee favoring J&K Bank Ltd, towards cost of RFP/bid security, details of the same is as under

No.:

Date:

Name of Issuing Bank:

Dated at _____this _____day of _____2026

We certify that we have provided all the information requested by the Bank in the format requested for. We also understand that the Bank has the exclusive right to reject this offer in case the Bank is of the opinion that the required information is not provided or is provided in a different format. It is also confirmed that the information submitted is true to our knowledge and the Bank reserves the right to reject the offer if anything is found incorrect.

We agree to all terms & conditions of the RFP.

Annexure K: Know Your Employee (KYE) Clause

Bidder has to submit Undertaking on company letter head as per format given below.

1. We on the behalf of _____ (name of the company) hereby confirm that all the resources (both on-site and off-site) working on the Bank's project i.e._____ _____ (Name of the RFP) have undergone KYE (Know Your Employee) process and all the required checks have been performed prior to employment of said employees as per our policy.
2. We confirm to defend and keep the bank indemnified against all loss, cost, damages, claim penalties expenses, legal liability because of non-compliance of KYE and of misconduct of the employee deployed by us to the Bank.
3. We further agree to submit the required supporting documents (Process of screening, Background verification report, police verification report, character certificate, ID card copy, educational document, etc.) to Bank before deploying officials in Bank premises for _____ (Name of the RFP)."

Sign and seal of Competent Authority
Name of Competent Authority
Dated

Annexure L: Service Level Agreement

This Service Level agreement ("Agreement") is made at Srinagar (J&K) on this ……. day of …….2026 between

i. "The Jammu and Kashmir Bank Ltd, a Banking Company under Indian Companies Act,2013 having corporate and registered office at M.A.Road,Srinagar,J&K,India-190001 represented herein by Authorized Signatory (hereinafter referred as **Bank** which unless the context requires include its successors in interests and permitted assigns) of the ONE PART, through its authorized signatory Mr.……

and

ii. M/S ……, registered under the …… Act, having its Registered Office at …… (Hereinafter referred to as the "Company" which expression shall unless it be repugnant to the context or meaning thereof, include its successors and assigns) of the OTHER PART, through its authorized signatory Mr.…….

The Bank and Company are hereinafter collectively referred to as 'Parties' and individually as a 'Party'.

Now therefore, this Agreement is witnessed as under:

Definitions of the terms

The Bank/J&K Bank:	Reference to the "the Bank", "Bank" and "Purchaser" shall be determined in context and may mean without limitation "The Jammu & Kashmir Bank".
Bidder/Vendor/Supplier:	An eligible entity/firm submitting a Proposal/Bid in response to this RFP.

Proposal/Bid:	The Bidder's written reply or submission in response to this RFP.
RFP:	The request for proposal (this document) in its entirety, inclusive of any addenda that may be issued by the Bank.
The Contract:	The agreement entered into between the Bank and the Company, as recorded in this Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
The Contract Price:	The price payable to the Company under the Contract for the full and proper performance of its contractual obligations.
The Product:	All of the software or software, all hardware, database, middleware, operating systems and/or other materials which the Company is required to supply to the Bank under the Contract.
System:	A Computer System consisting of all Hardware, Software, etc., which should work together to provide the services as mentioned in the Bid and to satisfy the Technical and Functional Specifications mentioned in the Bid.
Specified Bank Location:	Banks Data Centre located at Noida and Banks Disaster Recovery Site Located at Mumbai.
PBG:	Performance Bank Guarantee.
Data Centre (DC):	Banks Data Centre located at Noida.
Disaster Recovery (DR):	Banks Disaster Recovery Site located at Mumbai.
Material Breach:	Company failure to perform a major part of this Agreement.
Charges:	Commercials as per Purchase Order.
Confidential Information:	It includes all types of Information that will be found on BANK systems that the Company may support or have access to including, but are not limited to, Information subject to special statutory protection, legal actions,

	disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

Scope

The Bidder shall be responsible for supply, installation, implementation and management of the following modules as a part of the Centralized Endpoint and Server Protection Solution:

1. Enterprise Antivirus Solution/Endpoint Protection (EPP) with the following features
    a. Anti-Virus
    b. Anti-Malware
    c. Antispyware,
    d. File Reputation
    e. Exploit Prevention (host firewall, exploit protection)
    f. Command and Control (C&C) protection
    g. Zero-day Vulnerability Protection
    h. Device Control
    i. Ransomware Protection
    j. Desktop Firewall & Host Intrusion Prevention
    k. Browser IPS
    l. Application Control or File discovery
    m. Machine Learning-driven Exploit
    n. Network Integrity, Wi-Fi Reputation, and Smart VPN
    o. Active Directory Defence
    p. Active Directory Breach Assessment
    q. Adaptive Security
    r. Threat Intelligence API
    s. Isolation
    t. Mobile Threat Protection/Defence
    u. File Integrity Monitoring
2. Endpoint Detection & Response (EDR) and Extended Detection & Response (XDR)
3. Endpoint Encryption
4. Server Security

5. Setup and Implementation of the complete solution at DC and DR including Integration with various endpoints and security solutions.
6. The bidder should take care of Supply, Implementation, Maintenance and support of end point security solutions at all the endpoints and machines at all Bank's locations including branches, Cluster Offices, Zonal Offices etc. and which are connected to Bank's Data Center and DR through MPLS, Leased line, RF/VSAT, 4G/5G etc.
7. All the jobs / tasks / Blockade / application blacklist / whitelist etc. on present Application is to be incorporated along with necessary reports (success / failure of jobs etc.) on proposed Application.

Supply of Solution

1. The Bidder is required to design, size supply, implement & maintain the solution at Bank's DC and DR locations during the tenure of the contract. The supplied solution must be able to protect Bank's infrastructures such as Desktops, Laptops, Tablets, Servers, etc. at all the locations including Bank Branches, Circle offices and Zonal offices and other JK Bank's office locations.
2. The Bidder shall quote for the solution, which should be able to cater to more than 13 thousand endpoints for Bank. All the technical specifications and features as mentioned in the RFP must be deployed by the bidder. The solution should be further scalable to the adequate capacity as per the business requirements of the Bank.
3. The minimum server specifications for the solution to be proposed by the Bidder.
4. Below is the tentative requirement of the Bank. The initial tentative estimated requirement is of approx. 11500 licenses. In case of future requirement Bank shall place the additional order at same rates, terms and conditions.
5. The solution should take care of updating of antivirus on devices/endpoints in offices connected through MPLS VPN, Leased line, RF/VSAT, 4G/5G along with Servers at DC & DR Site.
6. The public Cloud based solutions should not be proposed under this RFP and if proposed, shall not be considered. Bidder should propose on-premises solution only for complete solution as per RFP.

7. The solution has to be installed each at DC (at present in Noida) and at DR (at present in Mumbai) in HA at each site. In addition, the solution should be capable to work in active-active mode between DC & DR with an option to shift/bifurcate the load at each location. The solution setup at DR should be an exact replica of the solution setup at DC i.e., configuration, security policy etc. must be in sync at each site DC & DR and if either fails, the other setup should be able to handle/cater the complete load. The bidder should ensure that there is no single point of failure in the solution at any point of time. In case Bank shifts it's DC and/or DR to any other location during the tenure of the contract, vendor shall be responsible for de-installation, re-installation and migration (if required) of the entire solution without any additional cost to the Bank. Transportation and insurance during such shifting activity shall be the responsibility of the Bank.
8. The bidder should setup the endpoint security solution for JK Bank in HA at each site (DC and DR) to ensure that JK Banks endpoints/devices are addressed as per RFP requirement.
9. All terms & conditions and Scope of work applicable for DC shall be applicable for DR as well. Any software required to synchronize DC setup & DR setup of this solution should be provided by the bidder.
10. The Bidder shall provide details of each hardware and software component such as number of licenses factored, make and model, specifications, license type, etc. and their price breakup of each component in the Commercial Price Bid on a separate sheet
11. No freeware or unlicensed/unsupported open-source software should be proposed as part of the solution and Bidder shall have to ensure the same.
12. The responsibility of Bidder shall be to maintain, manage and support including patches, updates and upgrades implementation of EPP, EDR & XDR across all JK Banks offices and branches.
    a. The Bidder must provide a mechanism to ensure regular updates of Antivirus Updates, patches, virus definitions on desktops and servers.
    b. The bidder should propose a solution, which should be flexible in deployment. Solution should be supported on-premises, cloud managed, and hybrid models.
    c. A single unified agent is mandatory for Anti-Virus, Anti-Malware, Antispyware, File Reputation, Exploit Prevention, Command and Control (C&C) protection, Zero-day Vulnerability Protection, Device Control, Ransomware Protection,

Desktop Firewall & Host Intrusion Prevention, Browser IPS, Application Control or File discovery, Active Directory Defence, Active Directory Breach Assessment, Adaptive Security, Threat Intelligence API, Isolation.

13. For all hardware/Appliances and software components, the bidder must provide 3 years warranty from the date of Go-Live of the solution at no extra cost to Bank.
14. The bidder shall ensure to quote 3 years subscription-based licenses for the complete solution as per RFP, and the period/tenure shall be start from the date of implementation.
15. Bidder should ensure that the quoted solution must be as per the scope and technical Specifications given in the RFP. Bidder should implement the solution at all the endpoints (i.e., at Zonal Offices, Cluster Offices, Branches and offices etc.) centrally from DC/DR location. Wherever installation is not feasible centrally, the bidder has to ensure the implementation of endpoint security at particular location manually/physically.
16. The proposed solutions shall be tightly integrated with all existing setup and new infrastructure /Assets of the Bank.
17. The solutions should be designed in such a way that they cover all the divisions of the Bank's Data Centre having separate networks & all separate network segments of each.
18. The proposed solution should be configured and scalable to cater the requirement of the Bank and the solution deployment should be compliant with Bank's IS, IT and Cyber policies, internal guidelines, regulatory requirements and country wide regulations and laws from time to time.
19. In case more than one device/appliance is provided to cater to the above requirements, then it should have the capability to sync all configuration between all devices in case changes are being made on one device from a single management console. In case the syncing requires any external device, the same has to be provided without any additional cost to the Bank.
20. The solution should effectively and efficiently manage operations and security posture of the Bank by preparing for and responding to cyber risks/threats, facilitate business continuity and recovery from cyber-attacks / incidents.
21. Any future upgrades and updates of software should be given free of cost and the solution should support any such upgrade during the contract period without affecting the performance of the solution.

22. The solution should be in adherence to the guidelines provided in the RBI cyber security circular no RBI/2015-16/418 dated 2nd June 2016 and its amendments (in present and in future) and guidelines, advisories. circulars from RBI and any statutory or regulatory body or Govt. of India from time to time. The bidder shall ensure all features and fine-tuning in the solution as per prevailing and future guidelines from RBI, GOI, other regulatory bodies and compliance on advisories from National Critical Information Infrastructure Protection Centre (NCIIPC), CERT-IN, CSITE and other statutory/Govt. bodies.
23. The bidder shall submit deployment methodology as part of project plan inline to the functional requirements of the solution.
24. The bidder should propose solution that identifies rogue Wi-Fi networks, utilizes hotspot reputation technology, and delivers a policy-driven VPN to protect network connections and support compliance.
25. The bidder should include features of EPP that blocks known network and browser-based malware attacks using rules and policies and prevents command and control setup with automated domain IP address blacklisting.
26. The solution should continuously probe Active Directory for domain misconfigurations, vulnerabilities, and persistence using attack simulations to identify risks and allow for immediate mitigation and remediation recommendations.
27. The solution should highlight anomalous sources of suspicious behaviour and reduce overall incident volume, enabling the SOC to focus on activity with the most potential for negative impact.
28. The solution should defend the primary attack surface for lateral movement and domain admin credential theft by controlling the attacker's perception of an organization's Active Directory resources from the endpoint using unlimited obfuscation (meaning fake asset and credential creation).
29. The solution should provide the ability to record and analyze endpoint behaviour to identify Advanced Attack Techniques that may be using legitimate applications for malicious purposes. This data should be enriched with the MITRE ATT&CK framework to help guide incidents responders during investigations.
30. The solution should hunt for high-fidelity incidents and combines the power of advanced machine learning and expert SOC analysts to discover the tools, tactics, and procedures used by adversaries. It should ensure that critical attacks are quickly identified with the

relevant context. In addition, it should deliver intuitive access to global security data to augment Bank's threat-hunting efforts.

31. The solution should provide recommendations for automatic policy tuning, adaptations and tasks to improve the security posture. The solution should be implemented centrally at all the endpoints with all the features and components mentioned in the RFP. Partial implementation shall not be accepted. Bank shall review the endpoint security implementation at any point of time before sign-off.
32. The solution should support autonomous security management that learns from admins, the organization, or the community to continuously assess and strengthen the security posture. It should also use Artificial intelligence (AI) guided management for establishing strong security policies with fewer misconfigurations and help improve overall security hygiene and posture.
33. The server security solution should support the most widely used server OS platforms which includes Microsoft Windows and non-Windows platform like Linux (Red Hat, Ubuntu, and Oracle), Solaris & AIX, etc.
34. The Server security solution shall have provision to provide protection against the vulnerabilities exploited by the threat actors.
35. All the patches, versions, upgrades, updates should be applied as and when released by the OEM throughout the contract period without any additional cost to the Bank.
36. Vendors should provide support during the entire period of the contract. In case there is a need to depute additional onsite engineers during any Issue, upgradation, updation process then the vendor has to ensure the same without any additional cost to the Bank. Further, online, telephonic, remote in addition to onsite support should be given for resolving operational issues.
37. The solution should be configured in High Availability (HA) at DC and DR along with Load Balancing functionality to cater the load equally or distribute the traffic on each system equally, if required bidder should factor any other software/hardware to perform the functionality with the solution without any additional cost to bank.
38. The bidder has to ensure that during the contract period, the solution utilization and server's CPU utilization should not exceed 70% and server's RAM utilization should not exceed 80%. In case the performance is adversely affected or the utilization of any server or any peripheral exceeds the mentioned threshold as above, more than 3 times

in a quarter, the vendor is required to upgrade the hardware or solution (as applicable), within one month without any additional cost to the Bank.

39. The Vendor should maintain Uptime of 99.95% monthly for the Solution during the contract period.
40. The solutions should be able to integrate various log types and logging options into SIEM and syslog. The solution should also have inherited feature for logging and alerts.
41. Integrate all the solutions with SIEM to generate alerts for any violations and provide a correlated view of threats and vulnerabilities associated with them along with remediation mechanism.
42. Scope of work applicable for DC will be applicable for DR as well. Any software required to sync DC setup & DR setup of EPP, EDR/ATP, XDR & Server Security solution should be provided by the bidder. The policy replication should be support over WAN also.
43. The EPP, EDR, XDR & Server Security solution should take care of bandwidth while updating of solutions on Desktops in branches connected through MPLS, VPN, Leased line, RF/VSAT, 4G/5G or any other technology Link along with Servers at DC & DR Sites.
44. Bidder should set up proper DC-DR replica configuration for Live Update on both Primary and Secondary Network link.
45. The responsibility of Bidder is to maintain/ manage/ support includes patches, updates and upgrades implementation of EPP, EDR, XDR & Server Security solution across all JK Bank branches, Cluster Office, Zonal Office at DC & DR Site.
46. JK Bank offices the Bidder must provide a mechanism to ensure regular updates of Antivirus Updates, patches, virus definitions on desktops and servers.
47. The Bidder has to ensure that the proposed EPP, EDR should be able to install its agents and send updates / patches and receive status on the available bandwidth during office hours without affecting the normal work of the office.
48. The monthly reports giving information like updated on endpoint / client, non-updated on endpoint clients, version details and any other reports specified by JK Bank should be provided to Head Office, Circle & Zonal, other Offices and branches.
49. In case any problem (bulk issues) occurs in any of the authorized software/application of JK Banks due to proposed solution, Bidder has to coordinate with JK Banks/ Application Vendor / AMC Vendor of JK Bank & resolve the same during the tenure of contract. In case such issue is attributed to the OEM/OSD of the solution, Bidder shall liaison with the OEM/OSD on priority and ensure deployment of corrective measures

through deployment of patches, upgrades, additional hardware as required without any additional cost to the Bank.

50. EPP, EDR, XDR Installation in the endpoint (Desktops/ Laptop), if any issue arises, the bidder's resource shall be responsible to coordinate with AMC partner and ensure resolution of all such issues. However, field support will be done by respective AMC vendors.
51. Bidder shall also submit procedural documents related to SOP, day to day operations, backup, periodic restoration, etc.
52. Bidder shall provide draft implementation plan of EPP, EDR, XDR & Server Security solution along with technical bid. The Bidder will also have to document the post install configuration and settings in a post install system configuration document.
53. Successful Bidder shall submit the detailed implementation strategy/ plan of EPP, EDR, XDR & Server Security solution vetted by respective OEM before implementation.
54. The proposed EPP, EDR, XDR & Server Security solution should be capable to sensitize Endpoints/ Servers etc. for not updated with latest updates and should have capability to allow/ not allow machines to connect into network unless latest updates are done in machine based on group policy of proposed solution.
55. The proposed solution should be capable of integrating with Desktop management solution and patch management solution, wherever applicable.
56. Bidder is also, required to supply, Install/Implement, Configure and Maintain the solution for the period of contract.
57. Bidder is required to provide ATS / AMC / subscription to maintain the same for the period of contract for the components part of this RFP.
58. Bidder should have back-to-back OEM and OSD support services for EPP, EDR, XDR & Server Security solution and all the associated hardware and software components.
59. The Bidder shall be responsible for management of this project and provide timely update to Bank.
60. The migration should be seamless with no or minimal disruption (if required). In case of any downtime required, the same may be made available to the Bidder only after prior approval from the Bank and after-business hours.
61. During the warranty (and Subscription Period) period and ATS, AMC, Subscription period, the bidder is bound to do all software and firmware upgrades, updates of proposed solution to next or required version without extra cost to the Bank, covering all parts

and labour from the date of acceptance of the systems by the Bank at the respective location i.e., on-site comprehensive warranty.

62. The bidder shall provide the solutions with complete features (over and above to technical specifications) without any extra cost to the Bank and all functionalities should be available for the Bank.
63. The bidder shall provide complete services for the applications under the scope including installation, implementation, integration, migration, management, maintenance, support (Update & Upgrade of Software and Hardware Firmware), audit compliance and knowledge transfer.
64. The bidder shall be responsible to migrate the existing technologies, if required, with new Proposed solution as per the technical specification along with all features.
65. The Bidder is required to design & size the EPP, EDR, XDR at DC and DR. Currently, Bank has about 11500 endpoints. Keeping in view the future growth, it is envisaged that the endpoints may increase to 20,000 at JK Bank during the tenure of 3 years.
66. The solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network.
67. The solution should include all components and subcomponents like software licenses, accessories, and the bidder should supply other components (if not specified) at no extra cost to the Bank that is required for commissioning of the solution as a part of RFP.
68. The bidder shall follow all respective technical/statutory guidelines, validations should be implemented, checked & verified, and related reports including SOP, Software Integrity Certificate and VAPT Clearance must be submitted, duly certified by OEM to the Bank for sign off the successful installation.
69. Post installation of Solution with its components including OS, VA & PT (Vulnerability Assessment & Penetration Testing) shall be conducted, and Bank InfoSec Team will provide a report to the Successful Bidder. All findings/issues pointed out in the report to be complied/fixed before commissioning and sign-off of the software (All components i.e., Database, application). The InfoSec Team and Other statutory authorities conduct review/ audit of the solutions time to time. All such Audit reports including VAPT Reports to be complied / attended by bidder/OEM within the timelines, during the entire period of contract also conduct periodic review audit of the database and application.

70. The solution deployment should be compliant with Bank's ISMS, IT and Cyber policies, internal guidelines, regulatory standards and countrywide regulations and laws from time to time.
71. The proposed EPP, EDR, XDR & Server Security solution should integrate with Bank's platforms like Security Operation Centre (SOC), Privileged Identity Management (PIM), and Security Incident Event Management (SIEM) (including SOAR or any other security solution implemented in Bank) to meet security and compliance requirements as and when required.
72. The bidder must submit detailed architecture of the provided solution/ every module along with installation and administration guide, which must include High-Level Design (HLD), and Low-Level Design (LLD) along with technical bid. Architecture Diagram of proposed & implemented solution as actual in the Bank environment.
73. The Proposed solution should be free from any kind of vulnerabilities and as and when vulnerabilities are notified by the auditor, Bank, regulators, Govt. of India and any other Govt. agencies, it should be patched within prescribed time with no cost to Bank during the contract period.
74. The bidder shall do regular backup of the solutions as per the defined Banks backup policy and solution should integrate the existing Banks Backup Solution.

Solution Implementation and Migration

The bidder shall coordinate with all solution providers/ vendors while installing and ensure installation and commissioning for running the application.

1. The Bidder shall be responsible to perform a clean uninstall of the existing Antivirus/ endpoint protection solution installed at the endpoints before installation of the new endpoint solution.
2. The bidder shall confirm the integrity of the software supplied i.e., the software is free from bugs, malware, covert channels in code etc. and Integrity certificate should be submitted to the Bank.
3. The production setup and solution architecture including Designing of complete solution, solution Flow architecture and Network Architecture should be designed & audited by the respective OEM(s)/OSD(s) of the Solution and its components and duly signed by respective OEM before the Final sign-off of the solution.

4. The successful bidder shall migrate all the data from existing EPP, EDR/ATP, XDR & Server Security solution in Bank to new Solutions procured through this RFP.
5. Solution should be able protect applications deployed on Docker, Containers & Virtual cloud for easy, deployment and building on premises if Bank decided to migrate to such setup in future.
6. The Proposed solution should be able to be deployed in Container form bundled into a single package consisting of all libraries, binaries, configuration and all its dependencies. It should be able to run independently irrespective of Operating System (OS) Distribution and underlying physical infrastructure. The bidder shall ensure that container deployment architecture should not limit the application performance, which would be otherwise available in non-container (traditional) deployment.
7. The proposed solution must have redundancy at all levels e.g., network redundancy (for management network interfaces) and power-supply redundancy at hardware/ software level required to achieve the high availability/ redundancy as per defined SLA/uptime.
8. Proposed solutions should have very high-scale architecture on a platform that scales efficiently. The solution should support 64-bit architecture environments for high scalability. Solution should support installation on Windows environment. Solutions should have extensible architecture for easy integration and automation.
9. Solution installation should support multiple-deployment options – Centralized, Distributed and hybrid deployments with option for a centralized operations console view (Dashboard).
10. The Bidder should provide customized (as per the requirement of the Bank) and pre-defined reports in HTML, CSV, Excel, PDF and other required file formats. All reports should be configured to generate auto or scheduled responses and send via SMTP on daily/monthly/yearly as per the Bank requirement at no additional cost to the Bank during the period of contract.
11. The proposed solution should be tightly integrated with all the existing other security tools / setup and new infrastructure /Assets of the Bank.
12. The selected bidder should implement and maintain this Solution for a period of 3 years including, Three (3) years Warranty from the date of final sign-off.
13. For implementation, Bidder should provide resources onsite to complete the implementation on time. A project manager must be deputed onsite during implementation phase at no additional cost to the Bank.

14. The bidders shall also provide the following documents, but not limited to, as part of the deliverables of the project.
    a. Original manuals of all proposed software/applications.
    b. Standard Operating Procedures for various activities such as administration, troubleshooting, regular health check-up, maintenance / clean-up activities etc.
    c. Installation & Technical Master Configuration Documents.
    d. Network & Security Design Documents (Will be approved by the Bank).
    e. Executive summary report for the project to the management fortnightly during implementation till go-live.
    f. Training materials.
15. Data security and Integrity to be ensure at rest as well as in transit.
16. The Bank shall give Bidder/OEM and its personnel only physical access to the support location and the designated hardware & equipment to enable Bidder to provide the maintenance & support services.
17. Bank will provide the Network access / availability for EPP, EDR & Server Security solution integration with Bank network at DR & DR. However, the required network sizing and other details has to be provided by the Bidder.
18. The solution should support the features and functionalities as mentioned in the Compliance to Technical & Functional Specifications of the Solution.

Onsite Technical Support

1. Post implementation the Successful bidder has to ensure the availability of support engineers at Bank's data centre for administration, operations, management and all activities related to the solution on all days of the week as well as beyond office hours, or whenever asked or needed.
2. Resident support engineer shall provide post implementation support at DR site remotely from DC, or visit to that site in case of need, without any additional cost to Bank.
3. Preventive maintenance of devices/ solution should be performed on quarterly basis at all locations for which solution is bought.
4. Overall management of the complete solution such as refinement of policies, creation of policies and database team during Databases creations, etc.

5. Proactive monitoring of health of the solution, including the H/W, S/W, application, solution on various parameters such as CPU, memory, storage, interface utilizations, etc. from Centralize Dashboard.
6. Health check for critical applications\ Workloads
7. Preparing and submitting reports as per the requirement of the Bank. Reports will include daily health monitoring and other statistical reports. If any report is available out of the box, then engineer has to customize the same as per the Bank's requirement with no extra cost to Bank. Engineer may take support from its Backend team and/or OEM if required.
8. Troubleshooting day-to-day issues, faced by end users, pertaining to proposed solution in coordination with Bank's Network integrator, security integrator, desktop management team or other relevant teams/vendors.
9. The Bidder shall provide requisite skilled resources during the implementation period during working hours and for post Implementation, the OTS resource for 24x7x365 from the date of Go-Live. Below are the minimum tentative resources and shift details for OTS (Onsite Technical Support):

Resource Type	Daily working hours	Minimum No. of resources to be present per day
L2	09:00AM to 6:00PM on Bank's Working days. The resources shall be responsible for JK Bank setup and endpoints	1

10. The onsite resources must be on bidder's payroll, subcontracting shall not be allowed of any resource(s) during the contract period.
11. Bidder may deploy additional resources to factor the week-off, leaves, compliance to labour and other applicable laws. Bank shall however bear the cost of the resources as per the quantity mentioned in the Purchase Order only.
12. All the resources deployed should have requisite knowledge and experience required for management and monitoring of the overall operations of all the implemented solutions.

13. Bidder is also required to provide a senior resource as and when required by the Bank, during the entire contract period of 3 years, for managing overall operations of the implemented solutions, without any extra cost to the Bank.
14. Bidder shall also provide one Team Lead for the entire duration of the project who shall be the SPOC for all issues and shall report onsite to the Bank on monthly basis for review.
15. Qualification of resource

Role/ Description	Experience	Educational Qualifications/Certifications/ Skills
L2	Minimum 5 Years	1. Good Communication (written/Oral) 2. Hands-on experience of Endpoint Security Solutions including EPP, EDR, Server Security etc. 3. The resource must be certified professional in the OEM technology.

Training

Bidder(s) must mandatorily provide training to the Bank Core team (Technical & Administrative). It is also the responsibility of the bidder to provide training manuals/SoP to each participant. All training material should be in English and should include Specific architecture and layout done for Bank. Training will be arranged in batches. The training should be provided onsite and remotely.

Upgrades and Updates

1. Bidder should ensure that any signature, patches and virus definition must be updated/installed immediately after release by the OEM/OSD to the solution and integrated endpoints.
2. The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Appliance provided free of cost during contract period. If, however, the upgrades and/or updates are not available or the solution(software) is declared End of Life/ /End of Support, Bidder has to upgrade the solution to an equivalent or higher solution without any additional cost to the Bank

3. The bidder should inform to the Bank if any new version, service pack, upgrade of the proposed solution is released by OEM, within seven (7) days of such release and deploy the upgraded solution and endpoints within 15 days of such release without any cost to the Bank covering all parts, labour and accessories at the respective locations (DC and DR) of the Bank during the period of the contract.
4. During the period of the contract, all upgrades, updates or requirements in hardware, software, licensing, implementation of upgrades, patches, version changes etc., due to whatsoever reason including but not limited to EOL(End-of-Life) or EOS(End-of-Support), shall be done by the bidder within stipulated time but not later than one month without any additional cost to the Bank. EOS/EOL solution will not be accepted and if any solution is declared EOS/EOL during the period of contract, the bidder shall upgrade with equivalent or higher specifications as stated above, at no additional cost to the Bank. The solution Infrastructure (hardware/software or both) provided by the successful bidder should not be declared end of sale within 2 years of sign off the project. If at all the solution Infrastructure (hardware/software or both) partly or fully, is declared end of sale within 2 years of sign off, the successful bidder must provide the upgraded version (hardware or both) free of cost, to the Bank. All hardware and software components of complete solution Infrastructure should be updated and maintained by the bidder during the entire tenure of the contract.

Besides, all the below mentioned activities fall under the Scope of work as well:

I. The Bidder shall inspect the equipment/software delivered by the OEM to ensure that the products delivered are as per the final order placed by the Bank and shall conduct a detailed inspection of the inventory.

II. The Bidder shall avail services of the OEM for deployment of required licenses as per the Scope of Work. The bidder should have back-to-back arrangement with the OEM so that Bank will be able to log a call with the OEM directly.

III. The selected bidder has to supply and install the license provided by OEM as per the timelines and SLA levels prescribed in the RFP.

The Bidder shall ensure proper support including Warranty / AMC / ATS for all Software / licenses / Support with regard to the Endpoint Detection & Response (EDR) Solution with

Advanced XDR Capabilities supplied / renewed as part of this RFP, during the period of contract.

Contract Uptime

a) The "**Downtime**" shall mean the time period when the Service/Application is not available as per the service standards of this SLA resulting failure. "**Failure**" is the condition that renders the solution not available to customers. "**Restoration**" is the condition when the Company demonstrates that the solution is in working order and the Bank acknowledges the same. It excludes the scheduled outages planned in advance and when Bank denies access to the Company Engineer for carrying out repair activities.

b) **Percentage down time"** shall mean the aggregate of downtime of the particular system during the quarter expressed as a percentage of total available time in a year i.e. 90 * 24 hours. Thus, if the aggregate downtime of System works out to 2 hours during a year then the percentage downtime shall be calculated as follows:

$$\frac{2 \times 100}{90 \times 24} = 0.09\%$$ (Considering days in a quarter as 90)

(A quarter is taken as a calendar quarter and number of days are actually number of days in each quarter)

c) **Uptime"**: The Company shall guarantee and ensure the following SLA's are met during the Contract Period of the Hardware/Software/License:

Service Window	24*7
Uptime Commitment	99.99%
Data Availability	100%

The "**Uptime**", for calculation purposes, equals to the Total number of hours of the day in a quarter, less Downtime in number of hours. Any part of hour is treated as full hour.

The percentage uptime is calculated on quarterly basis as follows:

(Total hours in a quarter - downtime hours within the quarter)

---------- * 100

Total hours in a quarter

(A quarter is taken as a calendar quarter and number of days are actually number of days in each quarter)

d) **"Response Time"** shall mean the interval from receipt of first information from Bank to the company, or to the local contact person of the Company by way of any means of communication informing them of the malfunction in System/Solution to the time Company Engineer attends the problem.

e) **"Restoration Time"** shall mean the period of time from the problem occurrence to the time in which the service returns to operational status. This may include temporary problem circumvention / workaround and does not necessarily include root cause removal.

f) **"Resolution Time"** shall mean the period of time from the problem occurrence to the time in which the root cause of the problem is removed and a permanent fix has been applied to avoid problem reoccurrence.

g) During Period of contract, Company will maintain the services as per SLAs.

i. Any bugs and enhancement in services shall be rectified immediately.
ii. Any requirements amendments/modifications required by bank will have to be carried out by the identified Company during the contract.

iii. The maximum response time for a support/complaint from the site shall not exceed time defined, else it will fall under penalty clause.

iv. Company shall solve the software problem immediately after reporting of the problem by the Bank to the Company

v. Any rectification required in the Application Software due to inherent bugs in the System Software/ off-the-shelf software shall also be rectified by the Company, at no additional

cost with timelines as defined in the SLA.

The Company shall guarantee an uptime of 99.99% during engagement, which shall be calculated on quarterly basis. The "**Uptime**", for calculation purposes, equals to the Total number of hours of the day in a quarter, less Downtime in number of hours. Any part of hour is treated as full hour.

Penalties shall be imposed in case of total uptime of Setup/Solution during the Contract period is less than the committed uptime. During the warranty period, for every drop of 5% than committed Uptime, warranty for the entire project shall be extended for 12 months. During the AMC period, for every drop of 5 % than committed Uptime, penalty of 2 % shall be applied. However, if the downtime percentage exceeds 10 % or if the number of downtime occurrences is more than 12 per year, the Bank shall be within its rights to invoke the Performance Bank Guarantee submitted by the Company in regards to the supply and maintenance etc. of the solution without any notice.

Uptime	Penalty
99.9 and above	**Nil**
95-99.8	**5%**
90-95	**10%**

Penalties shall also be applicable if the technical declines from the service provider are more than the threshold/ acceptable level of 2%.

Technical declines	Penalty/Quarter
2%	NA
2-3%	2% of the project Cost/Quarter
4-5%	3% of the project Cost/Quarter
5-8%	5% of the project Cost/Quarter
8-10%	10% of the project Cost/Quarter

Service Levels:

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Company

shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the Company shall be reviewed by Bank that shall:

- Regularly check performance of the Company against this SLA.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

Non-Availability: Is defined as, the service(s) is not-available as per levels below.

a. **Severity Level 1**: Is defined as, the Service is not available or there is a major degradation in performance of the system.

b. **Severity Level 2**: Is defined as, the service is available but the performance is degraded or there are intermittent failures and there is an urgent need to fix the problem to restore the service

c. **Severity Level 3**: Is defined as, the moderate degradation in the application performance. Has no impact on the normal operations/day-to-day working.

The violation of any of the above SLA's will attract a penalty as set out in the table below:

Severity Level	Response	Restoration	Resolution
Severity-1	1 hrs.	4 hrs.	1 day
Severity-2	1 hrs.	8 hrs.	2 days
Severity-3	1 hrs.	12 hrs.	3 days

Penalties for Non-Compliance to Restoration and Resolution Time:

Severity Level	Restoration Breach	Resolution Breach
Severity-1	15 days of AMC Cost for every 4 hrs. of delay in restoration	15 days of AMC Cost for every 1 day of delay in resolution
Severity-2	10 days of AMC Cost for every 12hrs of delay in restoration	10 days of AMC Cost for every 2 days of delay in resolution
Severity-3	5 days of AMC Cost for every 24 days delay in restoration	5 days of AMC Cost for every 3 days of delay in resolution

Penalty for Delayed Delivery:

Without prejudice to the rights of Bank to terminate this agreement/ the related purchase order, in case of the failure to deliver the solution/service within the stipulated timelines, penalty shall be levied for every 1 week delay beyond due date at the rate of 1% of the order value (in which delay has occurred) (inclusive of all taxes, duties, levies etc.), up to a maximum of 10 weeks form the original delivery date .If delay exceeds 10 weeks, bank may in its sole discretion and without being bound to do so, extend the date of delivery or can invoke PBG and cancel the entire contract. In the event of the Bank agrees to extend the date of delivery at the request of the Company, it is a condition precedent that the validity of the Performance Bank Guarantee submitted by the Company in regard to the supply and maintenance etc. of the solution shall be extended by further period as required by the Bank before the expiry of the original Bank Guarantee. Failure to do so will be treated as breach of contract.

Any component has not been delivered or if delivered is not operational, will be deemed / treated as non-delivery thereby excluding the Bank from all payment obligations under the terms of this contract. Partial delivery of products is not acceptable and payment for such products will not be made until full delivery is completed.

Contract Period

The Contract shall be effective from date of acceptance of PO and shall be valid till _____ , i.e 3 years from successful go live of the solution/Service (_____), unless or until terminated by Bank in accordance with the terms of

this SLA. Thereafter the contract may further extended if both parties wish to continue on the same terms and conditions subject to satisfactory performance of the service provider.

Warranty / AMC

The Warranty for the solution should be for the period of 1 year from the date of successful go live i.e. _____ till _____. There after the AMC shall be started for period of 2 years. The contract can be further extended if both parties wish to continue on same terms and conditions.

During the warranty and AMC period, the Bidder will have to undertake comprehensive support of the Software Solution supplied by the Bidder and all new versions, releases, and updates for all standard software to be supplied to the Bank at no additional cost. During the support period, the Bidder shall maintain the Software Solution to comply with parameters defined for acceptance criteria and the Bidder shall be responsible for all costs relating to labour, spares, maintenance (preventive and corrective), compliance of security requirements and transport charges from and to the Site (s) in connection with the repair/ replacement of the Software Solution, which, under normal and proper use and maintenance thereof, proves defective in design, material or workmanship or fails to conform to the specifications, as specified. During the support period, the vendor shall ensure that services of professionally qualified personnel are available for providing comprehensive on-site maintenance of the Software Solution and its components as per the Bank's requirements. Comprehensive maintenance shall include, among other things, day to day maintenance of the Software Solution as per the Bank's policy, reloading of firmware/software, compliance to security requirements, etc. when required or in the event of system crash/malfunctioning, arranging and configuring facility as per the requirements of the Bank, fine tuning, system monitoring, log maintenance, etc. The Bidder shall provide services of an expert engineer at locations wherever required, whenever it is essential. In case of failure of Software Solution, the Bidder shall ensure that Software Solution is made operational to the full satisfaction of the Bank within the given timelines. Warranty/ AMC for the system software/ off-the shelf software will be provided to the Bank as per the general conditions of sale of such software. Support would be offsite or on-site and comprehensive in nature and must have back to back support from the OEM/Vendor.

The vendor will warrant products against defects arising out of faulty design etc. during the specified support period. In the event of system break down or failures at any stage, protection available, which would include the following, shall be specified.

a. Diagnostics for identification of systems failures

b. Protection of data/ Configuration

c. Recovery/ restart facility d. Backup of system software/ Configuration

Prompt support shall be made available as desired in this RFP during the support period at the locations as and when required by the Bank. The Bidder shall be agreeable for on-call/on-site support during peak weeks (last and first week of each month) and at the time of switching over from DC to DR and vice-versa. No extra charge shall be paid by the Bank for such needs, if any, during the support period. Bidder support staff should be well trained to effectively handle queries raised by the customers/employees of the Bank. Updated escalation matrix shall be made available to the Bank once in each quarter and each time the matrix gets changed.

Exit Clause

The Bank reserves the right to cancel the contract in the event of happening one or more of the following conditions:

1. Failure of the successful bidder to accept the contract and furnish the Performance Bank Guarantee within 30 days from receipt of purchase contract.

2. Delay in delivery beyond the specified period.

3. Delay in completing implementation/customization and acceptance tests/ checks beyond the specified periods;

4. Seriou's discrepancy in functionality to be provided or the performance levels which have an impact on the functioning of the solution.

5. In addition to the cancellation of contract, Bank reserves the right to appropriate the damages through encashment of Bid Security /Performance Guarantee given by the Bidder. Bank reserves right to exit at any time after giving notice period of one month during the

contract period.

Payment Terms

The Company must accept the payment terms proposed by the Bank as proposed in this section. Payment shall be made in Indian Rupees.

The Company's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the bank. The payments shall be made after deducting applicable TDS from the date of receipt of valid claims that are supported by original invoice, original Proof of Delivery (POD), acceptance by the bank and upon fulfilment of other conditions stipulated in the contract. The invoices and other documents are to be duly authenticated by Company. The Company therefore has to furnish the bank account number to where the funds have to be transferred for effecting payments.

Payments as per the schedule given below will be released only on acceptance of the order and on signing the SLA / NDA by the selected Company.

The Bidder must accept the payment terms proposed by the Bank as proposed in this section.

The Payments shall be made on the achievement of the following project milestones:

Project Milestone	Payment (Incl. Of applicable taxes)
On delivery of Hardware (If applicable)/ Installation of EDR with Advanced XDR Capabilities Solution and followed by activation of licenses subject to receiving UAT sign off & confirmation from JK Bank	40% of First year License cost
On Deploying policies and post Go Live Sign off as per JK Bank's requirement	60% of First year License cost
Payments shall be made for 2nd & 3rd Year	100% Yearly post rendering of services

All Payments will be done post confirmation from the Bank Teams.

Payment terms: -

1. Rates to be quoted exclusive of GST. The quantity mentioned above is indicative only and the actual number may change based on assessment of business requirements of the Bank.
2. Invoices to be raised after submission of 5% PBG of the total project cost & execution of NDA & SLA with the Bank.
3. All other terms and conditions as per RFP.

Assignment

The Company shall not assign, in whole or in part, the benefits or obligations of the contract to any other person without the prior written consent of the Bank. However, the Bank may assign any of its rights and obligations under the Contract to any of its affiliates without prior consent of the Company.

Entire Agreement, Amendments, Waivers.

i. This Master Agreement and each Service Attachment contains the sole and entire agreement of the parties with respect to the entire subject matter hereof, and supersede any and all prior oral or written agreements, discussions, negotiations, commitment, understanding, marketing brochures, and sales correspondence and relating thereto. In entering into this Master Agreement and each Service Attachment each party acknowledges and agrees that it has not relied on any express or implied representation, or other assurance (whether negligently or innocently made), out in this Master Agreement and each Service Attachment. Each party waives all rights and remedies which, but for this Section, might otherwise be available to it in respect of any such representation (whether negligently or innocently made), warranty, collateral contract or other assurance.

ii. Neither this Master Agreement nor any Service Attachment may be modified or amended except in writing and signed by the parties.

iii. No waiver of any provisions of this Master Agreement or any Service Attachment and no consent to any default under this Master Agreement or any Service Attachment shall be effective unless the same shall be in writing and signed by or on behalf of the party against whom such waiver or consent is claimed. No course of dealing or failure of any

party to strictly enforce any term, right or condition of this Master Agreement or any Service Attachment shall be construed as a waiver of such term, right or condition. Waiver by either party of any default other party shall not be deemed a waiver of any other default.

Severability

If any or more of the provisions contained herein shall for any reason be held to be unenforceable in any respect under law, such unenforceability shall not affect any other provision of this Master Agreement, but this Master Agreement shall be construed as if such unenforceable provisions or provisions had never been contained herein, provided that the removal of such offending term or provision does not materially alter the burdens or benefits of the parties under this Master Agreement or any Service Attachment.

Remedies Cumulative

Unless otherwise provided for under this Master Agreement or any Service Attachment, all rights of termination or cancellation, or other remedies set forth in this Master Agreement, are cumulative and are not intended to be exclusive of other remedies to which the injured party may be entitled by law or equity in case of any breach or threatened breach by the other party of any provision in this Master Agreement. Use of one or more remedies shall not bar use of any other remedy for the purpose of enforcing any provision of this Master Agreement.

Partnership / Collaboration / Subcontracting

The services offered to be undertaken in response to this RFP shall be undertaken to be provided by the company directly and there shall not be any sub-contracting without prior written consent from the Bank. Bank will only discuss the solution with company's authorized representatives. The company authorized representatives shall mean their staff. In no circumstances any intermediary (which includes Liasoning Agents, marketing agents, commission agents etc.) should be involved during the course of project. No subletting of the contract by the will be allowed under any circumstances. Neither the subject matter of the contract nor any right arising out of the contract shall be transferred, assigned or delegated to any third party by Vendor without prior written consent of the Bank.

Confidentiality

All the Bank's product and process details, documents, data, applications, software, systems, papers, statements and business/customer information etc. (hereinafter referred to as 'Confidential Information') which may be communicated to or come to the knowledge of the Company and /or its employees during the course of discharging their obligations shall be treated as absolutely confidential and the Company and its employees shall keep the same secret and confidential and not disclose the same, in whole or in part to any third party nor shall use or allow to be used any information other than as may be necessary for the due performance by the Company of its obligations. The Company shall

indemnify and keep Bank indemnified safe and harmless at all times against all or any consequences arising out of any breach of this undertaking regarding Confidential Information by the Company and/or its employees and shall immediately reimburse and pay to the Bank on demand all damages, loss, cost, expenses or any charges that Bank may sustain suffer, incur or pay in connection therewith.

It is clarified that "Confidential Information" includes any and all information that is or has been received by the Company (Receiving Party) from the Bank (Disclosing Party) and that (a) relates to the Disclosing Party and (b) is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential (c) is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agent, representatives or consultants.

In maintaining confidentiality, the Receiving Party on receiving the confidential information and material agrees and warrants that it shall take at least the same degree of care in safeguarding such confidential information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent any inadvertent disclosure. The Receiving Party shall also, keep the confidential information and confidential materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third Party.

The Receiving Party, who receives the confidential information and the materials, agrees that on receipt of a written demand from the Disclosing Party, they will immediately return all

written confidential information and materials and all copies thereof provided to and which is in Receiving Party's possession or under its custody and control.

The Receiving Party to the extent practicable shall immediately destroy all analysis, compilation, notes studies memoranda or other documents prepared by it which contain, reflect or are derived from confidential information relating to the Disclosing Party AND shall also immediately expunge any confidential information, word processor or other device in its possession or under its custody & control, where after it shall furnish a Certificate signed by the Authorized person confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries, the requirement of confidentiality aspect has been complied with.

The restrictions mentioned hereinabove shall not apply to: -

(a) any information that publicly available at the time of its disclosure; or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same; or

(b) any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any government, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosures, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.

The confidential information and material and all copies thereof, in whatsoever form shall at all the times remain the property of the Disclosing Party and disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document. The confidentiality obligations shall be observed by the Company during the term of this Agreement and thereafter and shall survive the expiry or termination of this Agreement between the Bank and Company.

The Company understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause BANK irreparable harm, may leave BANK

with no adequate remedy at law and as such the Bank is entitled to proper indemnification for the loss caused by the Company. Further the BANK is entitled to seek to injunctive relief besides other remedies available to it under law and this Agreement.

Information Security

a. The Bidder and its personnel shall not carry any written material, layout, diagrams, floppy diskettes, hard disk, flash / pen drives, storage tapes or any other media out of J&K Bank's premises without written permission from J&K Bank.

b. The Bidder's personnel shall follow J&K Bank's information security policy and instructions in this regard.

c. The Bidder acknowledges that J&K Bank 's business data and other proprietary information or materials, whether developed by J&K Bank or being used by J&K Bank pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to J&K Bank; and the Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Bidder to protect its own proprietary information. Bidder recognizes that the goodwill of J&K Bank depends, among other things, upon the Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Bidder could damage J&K Bank. By reason of Bidder's duties and obligations hereunder, Bidder may come into possession of such proprietary information, even though the Bidder does not take any direct part in or furnish the Service(s) performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by the Contract/Agreement. Bidder shall use such information only for the purpose of performing the Service(s) under the Contract/Agreement.

d. Bidder shall, upon termination of the Contract/Agreement for any reason, or upon demand by J&K Bank, whichever is earliest, return any and all information provided to Bidder by J&K Bank, including any copies or reproductions, both hardcopy and electronic.

e. That the Company and each of its subsidiaries have taken all technical and organizational measures necessary to protect the information technology systems and Data used in

connection with the operation of the Company's and its subsidiaries' businesses. Without limiting the foregoing, the Company and its subsidiaries have used reasonable efforts to establish and maintain, and have established, maintained, implemented and complied with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or Data used in connection with the operation of the Company's and its subsidiaries' businesses.

f. The Bidder shall certify that to the knowledge of the Bidder, there has been no security breach or other compromise of or relating to any information technology and computer systems, networks, hardware, software, data, or equipment owned by the Bidder or its subsidiaries or of any data of the Bidder's, the Operating Partnership's or the Subsidiaries' respective customers, employees, suppliers, vendors that they maintain or that, to their knowledge, any third party maintains on their behalf (collectively, "IT Systems and Data") that had, or would reasonably be expected to have had, individually or in the aggregate, a Material Adverse Effect, and

g. That the Bidder has not been notified of, and has no knowledge of any event or condition that would reasonably be expected to result in, any security breach or other compromise to its IT Systems and Data;

h. That the Bidder is presently in compliance with all applicable laws, statutes, rules or regulations relating to the privacy and security of IT Systems and Data and to the protection of such IT Systems and Data from unauthorized use, access, misappropriation or modification. Besides the Bidder confirms the compliance with Banks Supplier Security Policy.

i. That the Bidder has implemented backup and disaster recovery technology consistent with generally accepted industry standards and practices.

j. That the Bidder and its subsidiaries IT Assets and equipment, computers, Systems,

Software's, Networks, hardware, websites, applications and Databases (Collectively called IT systems) are adequate for, and operate and perform in all material respects as required in connection with the operation of business of the Bidder and its subsidiaries as currently conducted, free and clear of all material bugs, errors, defects, Trojan horses, time bombs, malware and other corruptants.

k. That the Bidder shall be responsible for establishing and maintaining an information security program that is designed to:

l. Ensure the security and confidentiality of Customer Data, Protect against any anticipated threats or hazards to the security or integrity of Customer Data, and

m. That the Bidder will notify Customer of breaches in Bidder's security that materially affect Customer or Customer's customers. Either party may change its security procedures from time to time as commercially reasonable to address operations risks and concerns in compliance with the requirements of this section.

n. The Bidder shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of Personal Data and/or use, access, copying, exhibition, transmission or removal of Bank's Confidential Information from Companies facilities. Bidder shall promptly provide Bank with written descriptions of such procedures and policies upon request. Bank shall have the right, upon reasonable prior written notice to Bidder and during normal business hours, to conduct on-site security audits or otherwise inspect Companies facilities to confirm compliance with such security requirements.

o. That Bidder shall establish and maintain environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss or alteration of the Client Data, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are no less rigorous than those maintained by Bidder for its own information or the information of its customers of a similar nature.

p. That the Bidder shall perform, at its own expense, a security audit no less frequently than annually. This audit shall test the compliance with the agreed-upon security standards and procedures. If the audit shows any matter that may adversely affect Bank, Bidder shall disclose such matter to Bank and provide a detailed plan to remedy such matter. If the audit does not show any matter that may adversely affect Bank, Service Provider shall provide the audit or a reasonable summary thereof to Bank. Any such summary may be limited to the extent necessary to avoid a breach of Bidder's security by virtue of providing such summary.

q. That Bank may use a third party or its own internal staff for an independent audit or to monitor the Bidder's audit. If Bank chooses to conduct its own security audit, such audit shall be at its own expense. Bidder shall promptly correct any deficiency found in a security audit.

r. That after providing 30 days prior notice to Bidder, Bank shall have the right to conduct a security audit during normal business hours to ensure compliance with the foregoing security provisions no more frequently than once per year. Notwithstanding the foregoing, if Bank has a good faith belief that there may have been a material breach of the agreed security protections, Bank shall meet with Bidder to discuss the perceived breach and attempt to resolve the matter as soon as reasonably possible. If the matter cannot be resolved within a thirty (30) day period, the parties may initiate an audit to be conducted and completed within thirty (30) days thereafter. A report of the audit findings shall be issued within such thirty (30) day period, or as soon thereafter as is practicable. Such audit shall be conducted by Bidder's auditors, or the successors to their role in the event of a corporate reorganization, at Bidder's cost.

Termination of Contract

If the Termination is on account of failure of the Successful Bidder to perform the obligations under this agreement, the Bank shall have the right to invoke the Performance Bank Guarantee(s) given by the selected bidder. The Bank will be entitled to terminate this Contract, on the happening of any one or more of the following:

For Convenience: BANK by written notice sent to the Company may terminate the contract in whole or in part at any time for its convenience giving 30 days prior notice.

In the event of termination of the Agreement for the Bank's convenience, Service Provider

shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

For Insolvency: BANK may at any time terminate the contract by giving written notice to the Company, if the Company becomes bankrupt or insolvent.

For Non-performance: BANK shall have the right to terminate this agreement or/and to cancel the entire or unexecuted part of the related Purchase Order forthwith by a written notice in the event the company fails to deliver and/or install the solution within the stipulated time schedule or any extension, if any, thereof agreed by the Bank in writing in its sole discretion OR the Company fails to maintain the service levels prescribed by BANK in scope of work OR fails to discharge or commits breach of any of its obligations under this Agreement.

In the event of termination, the company shall compensate the Bank to the extent of loss suffered by the Bank on account of such termination provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to BANK. The Bank shall inter-alia have a right to invoke the Performance Bank Guarantee submitted by the Company in regard to the supply and maintenance etc. of the solution for realizing the payments due to it under this agreement including penalties, losses etc.

Exit Clause

The Bank reserves the right to cancel the contract in the event of happening one or more of the following conditions:

1. Failure of the successful bidder to accept the contract and furnish the Performance Bank Guarantee within 30 days from receipt of purchase contract.

2. Delay in delivery beyond the specified period.

3. Delay in completing implementation/customization and acceptance tests/ checks beyond the specified periods;

4. Seriou's discrepancy in functionality to be provided or the performance levels which have an impact on the functioning of the solution.

5. In addition to the cancellation of contract, Bank reserves the right to appropriate the

damages through encashment of Bid Security /Performance Guarantee given by the Bidder. Bank reserves right to exit at any time after giving notice period of one month during the contract period.

Indemnity

The Successful bidder shall indemnify and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings (including attorney fees), relating to or resulting from: -

i. Intellectual Property infringement or misappropriation of any third-party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.

ii. Claims made by the employees who are deployed by the Successful bidder.

iii. Breach of confidentiality obligations by the Successful bidder,

iv. Negligence (including but not limited to any acts or omissions of the Successful bidder, its officers, principals or employees) or misconduct attributable to the Successful bidder or any of the employees deployed for the purpose of any or all of the its obligations,

v. Any loss or damage arising out of loss of data;

vi. Bonafide use of deliverables and or services provided by the successful bidder;

vii. Non-compliance by the Successful bidder with applicable Laws/Governmental/Regulatory Requirements.

The Successful bidder shall be responsible for any loss of data, loss of life etc. due to acts of its representatives, and not just arising out of negligence or misconduct, as such liabilities pose significant risk.

It is hereby agreed that the above said indemnity obligations shall apply notwithstanding anything to the contrary contained in this Tender document and subsequent Agreement and shall survive the termination of the agreement for any reason whatsoever. The Successful bidder will have sole control of its defense and all related settlement negotiations

Right to Audit

"Bank reserves the right to conduct an audit/ ongoing audit of the Company/Service Provider(including its sub-contractors).The Company shall be subject to annual audit by internal/ external Auditors appointed by the Bank / inspecting official from the RBI or the persons authorized by RBI or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and company is required to submit such certification by such Auditors to the Bank.

Company shall allow the Bank and RBI or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Company within a reasonable time failing which Company will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank."

Limitation of Liability

Neither Party shall be liable for any indirect damages (including, without limitation, loss of revenue, profits, and business) under this agreement and the aggregate liability of Company, under this agreement shall not exceed more than the total contract value.

Relocation and Shifting

The relocation / Shifting, if any required, of all the quoted components shall be done by the Bank at its own cost and responsibility. However, the Company shall supervise the de-installation and packing at the original site and re-installation at the new sites free of cost. The quoted components shall continue to remain within the scope of warranty for the transit period.

Force Majeure

i. The Selected Company shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

ii. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractor's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, pandemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.

iii. Unless otherwise directed by the Bank in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

iv. In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and the contractor shall hold consultations in an endeavor to find a solution to the problem.

v. Notwithstanding above, the decision of the Bank shall be final and binding on the successful Company regarding termination of contract or otherwise

Intellectual Property Rights

1.1 Bank as part of this Agreement, Company shall have right to use as well as right to license such technology/ software / product. The Bank shall not be liable for any license or IPR violation on the part of Company.

1.2 Without the Bank's prior written approval, Company will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank's rights under this Agreement.

1.3 Company shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.

1.4 The Bank will give (a) notice to Company of any such claim without delay/provide reasonable assistance to Company in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Company shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Company shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Company shall consult with the Bank with respect to the defence and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses by counsel of its own selection.

1.5 Company shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Company's compliance with the Bank's specific technical designs or instructions (except where Company knew or should have known that such compliance was likely to result in an Infringement Claim and

Company did not inform the Bank of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

Corrupt and Fraudulent practice

i. It is required that Company observe the highest standard of ethics during the procurement and execution of such contracts and not to indulge in any corrupt and fraudulent practice.

ii. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.

iii. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

iv. The Bank reserves the right to reject a proposal for award if it determines that the Company recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

v. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it becomes known that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

Governing Laws and Dispute Resolution

This agreement shall be governed in accordance with the Laws of UT of J&K read with laws of India so far as they are applicable to the UT of J&K for the time being and will be subject to the exclusive jurisdiction of Courts at Srinagar with exclusion of all other Courts.

The Bank and the Company shall make every effort to resolve any disagreement or dispute amicably, arising in connection with the Contract, by direct and informal negotiation between

the designated Officer of the Bank for .... and designated representative of the Company. If designated Officer of the Bank for ....and representative of the company are unable to resolve the dispute within reasonable period, which in any case shall not exceed_____ they shall immediately escalate the dispute to the senior authorized personnel designated by the Bank and the Company respectively. If even after elapse of reasonable period, which in any case shall not exceed _____, the senior authorized personnel designated by the Bank and the Company are unable to resolve the dispute amicably OR any party fails to designate its officer/representative/ senior authorized personnel within days from the date of request in writing for the same by the other party for amicable settlement of dispute, the dispute shall be referred to arbitration.

All disputes/differences which may arise between the parties shall be resolved mutual and amicable settlement between the parties within 30 days from the date of receipt of a written notice raising such dispute by either of the party. In case there is no amicable settlement between the parties, the dispute or difference arising in relation to meaning or interpretation of terms and conditions, the same shall be referred to a sole arbitrator to be appointed by Bank. The Arbitration and Conciliation Act, 1996 will be applicable to the arbitration proceeding and the venue of the arbitration shall be at Srinagar. The language of the arbitration proceedings shall be in English. The award of the arbitrator shall be final and binding. The courts at Srinagar shall have exclusive jurisdiction at Srinagar.

Notices

Unless otherwise provided herein, all notices or other communications under or in connection with this Agreement shall be given in writing and may be sent by personal delivery or by post or courier or facsimile or e- mail to the address below, and shall be deemed to be effective if sent by personal delivery, when delivered, if sent by post, three days after being deposited in the post and if sent by courier, two days after being deposited with the courier, and if sent by facsimile, when sent (on receipt of a confirmation to the correct facsimile number) and if sent by e-mail (on receipt of a confirmation to the correct email)

Following shall be address of BANK for notice purpose:

Chief Information Security Officer
Information Security Department.

Corporate Headquarters

The Jammu & Kashmir Bank

M.A. Road, Srinagar, Jammu & Kashmir (India) - 190001.

Following shall be address of Company for notice purpose:

_____

_____

_____

_____

Other Terms and Conditions

i. If any provision of this agreement or any document, if any, delivered in connection with this agreement is partially or completely invalid or unenforceable in any jurisdiction, then that provision shall be ineffective in that jurisdiction to the extent of its invalidity or unenforceability. However, the invalidity or unenforceability of such provision shall not affect the validity or enforceability of any other provision of this agreement, all of which shall be construed and enforced as if such invalid or unenforceable provision was/were omitted, nor shall the invalidity or unenforceability of that provision in one jurisdiction affect its validity or enforceability in any other jurisdiction. The invalid or unenforceable provision will be replaced in writing by a mutually acceptable provision, which being valid and enforceable comes closest to the intention of the Parties underlying the invalid or unenforceable provision.

ii. Bank reserves the right to conduct an audit/ ongoing audit of the services provided by Company. The Company agrees and undertakes to allow the Bank or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by the Company within a reasonable time failing which Bidder will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. The Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank.

iii. The company, either by itself or through its group companies or Associates, shall not use the name and/or trademark/logo of Bank, in any sales or marketing publication or

advertisement, or in any other manner.

iv. Any addition, alteration, amendment, of this Agreement shall be in writing, signed by both the parties.

v. The invalidity or unenforceability for any reason of any covenant of this Agreement shall not prejudice or affect the validity or enforceability of its other covenants. The invalid or unenforceable provision will be replaced by a mutually acceptable provision, which being valid and enforceable comes closest to the intention and economic positions of the Parties underlying the invalid or unenforceable provision.

vi. Each party warrants that it has full power and authority to enter into and perform this Agreement, the respective executants are duly empowered and/or authorized to execute this Agreement, and performance of this Agreement will not result in breach of any provision of the Memorandum and Articles of Association or equivalent constitutional documents of the either party or any breach of any order, judgment or agreement by which the party is bound.

vii. The terms and conditions laid down in the RFP shall be read and construed forming part of this service level agreement. In an event of contradiction on any term or condition between RFP and service level agreement, the terms and conditions of service level agreement shall prevail.

In witness whereof the parties have set their hands on this agreement in duplicate through their authorized signatories on the day, month and year first herein above mentioned.

Agreed and signed on behalf of	Agreed and signed on behalf of
Company's Authorized Signatory	J&K Bank Limited
Name……	Name……
Designation……	Designation……
Witness (1):	Witness (1):

Name.....	Name.....
Designation.....	Designation.....
Witness (2):	Witness (2):
Name.....	Name.....
Designation.....	Designation.....