Online RFP

For

Selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)

e- RFP Ref. No: JKB/CHQ/T&D/DC-Management/2025-1535
Dated: 13-10-2025

SCHEDULE OF RFP

e-RFP Reference No.	**JKB/CHQ/T&D/DC-Management/2025-1535 Dated: 13-10-2025**
Date of Issue of RFP	**15-10-2025**
RFP Description	**Selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)**
Issuer of the RFP-Department	**Technology & Development Department**
Bank's Communication Details	**J&K Bank Technology & Development, 5th Floor , Corporate Headquarters M.A Road , Srinagar**
RFP Application Fee (Non – Refundable)	**Rs.5,000/-(Rupees Five Thousand Only)) to be deposited through Transfer / NEFT to the below detailed 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**
Earnest Money Deposit (EMD) (Refundable)	**Rs.1,25,00,000/- (Rupees One Crore Twenty Five Lacs Only) to be deposited through transfer / NEFT to the following A/c with Bank details given as: 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 (EMD is exempted for all Start-ups as recognized by DPIIT/DIPP)**
Performance Bank Guarantee	**5% of total contract Value**
Bid Document Availability including changes/amendments, if any to be issued	**Document can be downloaded Bank's e-Tendering Service Portal https://jkbank.abcprocure.com/w.e.f October 15, 2025 16.00 Hrs. to November 14, 2025 17.00 Hrs.**

Last date for pre-Bids queries & submission Mode	on-line through the prescribed e-Tendering portal https://jkbank.abcprocure.com October 28, 2025 17.00 Hrs.
Pre-bid Queries Response date	All communications regarding points / queries requiring clarifications shall be given online on November 06, 2025
Pre Bid Meeting	Prebid Meeting shall be held online through Banks Online Meeting Platform. Bidders to submit a maximum of 2 Participants names, Contact Numbers, Designations and email ids on mail id:mir.farhat@jkbmail.com by the date of prebid query submission. Meeting invite link shall be sent by Bank to the bidder's email id.
Last date and time for Bid	November 14, 2025 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
Corrigendum	All the Corrigendum will be uploaded on online tender portal https://jkbank.abcprocure.com only
For e-Tender related Queries	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:

Sr. No	Name
1	Sandhya Vekariya – 6352631968
2	Suraj Gupta – 6352632310
3	Ijlalaehmad Pathan – 6352631902
4	Imran Sodagar - 9328931942

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 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.

List of Abbreviations

DC	**Data Centre**
DR	**Disaster Recovery**
HA	**High Availability**
BG	**Bank Guarantee**
OEM	**Original Equipment Manufacturer**
PBG	**Performance Bank Guarantee**
SP	**Service Provider**
EMD	**Earnest Money Deposit**
SLA	**Service Level Agreement**
NDA	**Non-Disclosure Agreement**
SI	**System Integrator**
TCO	**Total Cost of Ownership**
TCV	**Total Contract Value**
PO	**Purchase Order**
RFP	**Request For Proposal**
KYC	**Know Your Customer**
RoI	**Rest of India**
OS	**Operating System**
IP	**Internet Protocol**
CBS	**Core Banking Solution**
NLS	**Bank's Near Line Site**
EOL	**End of Life**
EoS	**End of Support**
TAT	**Turn Around Time**
SPOC	**Single Point of Contact**
NAP	**Network Access Point**
PM	**Preventive Maintenance**
MSP	**Managed Service Provider**
OEM	**Oracle Enterprise Manager**
Material Breach	**Bidder failure to perform a major part of this Agreement.**

SECTION A - INTRODUCTION

1. 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. 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://www.jkbank.com

2. Purpose of RFP

J&K Bank invites bids from eligible and experienced service providers for the SLA-based outsourcing of Data Centre Management Services at its Primary Data Centre (DC), Near Line Site (NLS) and Disaster Recovery Site (DR). The engagement shall ensure uninterrupted, secure, and compliant operations of the Bank's mission-critical IT infrastructure in line with regulatory guidelines issued by RBI, IT Act 2000, ISO 27001, Master directions on IT Outsourcing , and other applicable standards.

The objective of this RFP is to select a Bidder for providing SLA based Managed Services to support the Datacentre operations, Infrastructure Monitoring, Security, Administration and maintenance of the Bank's Data Center Facility at Noida, Near Line Site in Noida and DR Site located in Mumbai for a period of 5 years as per Scope of work given in this document.

This includes end to end management & operations of services and support on Servers, Databases, Middleware, Operating Systems (OS), Containerized Environments and Virtualization, Microsoft based AD/DNS and mail Messaging Hybrid Setup, Load Balancers, HSMs, Storages & Backup and other related infrastructure and allied components.

The selected MSP shall plan, design/re-design, implement, upgrade, operate and optimize all the software, solutions, assets and applications under scope. The MSP shall also be responsible to operationalize a process to ensure alignment with IT infrastructure and application life cycle management process.

The selected Managed Service Provider (MSP) will ensure the continued efficient functioning of all 3 sites of the Bank and provide essential support services within defined SLAs to avoid termination of contract or levying of penalty/ Liquidated damages or any legal action . The bidder must comply with the terms and conditions outlined in this RFP.

Bidder must have previous experience/competency in similar kind of engagements serving Scheduled Commercial Banks / PSU Banks in India for minimum 3 years and having support centres in different locations in India with high availability to provide the desired support to the bank within defined SLAs . The selected Managed Service Provider (MSP) has to provide, manage and maintain all necessary infrastructure components and services that would be necessary as per the defined requirements of the RFP. The selected Bidder has to ensure that the desired objectives of this RFP are fulfilled.

The bidder shall appoint a project manager (PMO) for managing day-to-day activities including but not limited to shift schedule only. The appointed PMO shall be responsible for publishing the activity tracker to Bank at agreed intervals. L1, L2 & L3 resources shall be strictly on the payroll of bidder. However, L1 Technical Support from Authorized Service Delivery Partners for not more than 20% shall be allowed with prior approvals from the Bank Team, however in such a case also, the overall SLA ownership shall remain with the bidder only. Not more than 25 resources at DC Site and 4 at DR Site would be deployed in a shift by the MSP, as per the shift schedule intimated to the Bank. Main shift shall be from 09:00am to 06:00pm for all days (excluding Monthly/Quarterly/Yearly Closings wherein expert resources of all domains need to be present on 24x7 basis).

Any change with regards to the resource or resource shift as may be highlighted by the Bank should be prioritized and complied. MSP shall ensure deployment of ample resources in each shift as agreed with the Bank.

3. Eligibility Criteria

J&K Bank shall scrutinize the Eligibility bid submitted by the bidder(s). A thorough examination of supporting documents along with Onsite/virtual meetings with the client references to meet each eligibility criteria (Annexure D) shall be conducted to determine the Eligible & Technically qualified 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 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 & client satisfaction reports a bidder can provide. Bank at its own discretion can conduct the Onsite/virtual meetings with the client references to ascertain the

4. High Level Scope of Work

Scope of work of the Managed services engagement as desired in this RFP shall be Management and Operations of Entire DC, DR and NDC/NLS Activities which include Plan, Design, Implement, operate, optimize and retirement phases of IT Management Lifecycle on 24x7 basis for a period of minimum 5 years. The MSP shall also be responsible to operationalize a process to ensure alignment with IT infrastructure and application life cycle management process. The broad scope of work includes but is not limited to the following:

1. Management, Monitoring & Administration of:
    i. Physical Servers & Virtual Machines with associated storages & mount points.
    ii. Virtualizations
    iii. Operating Systems
    iv. Databases
    v. Middlewares
    vi. Containerized Environments (OCP/OKE)
    vii. Storage & Backups- Allocation, Recovery & Restoration
    viii. Tape Library/Media Management
    ix. Load Balancer & HSMs - configuration, management and administration. (F5/Citrix/Radware/A10)
    x. AD/DNS (*DNS/Proxy issues should be carried out centrally/remotely through respective tools/software*)
    xi. Exchange Mail System
    xii. Physical Server Hardware (excluding hardware maintenance and replacements) & Assets in Bank's Cage Areas at all 3 sites of the Bank.
    xiii. Cloud/SaaS based Infrastructure (AWS, AZURE, OCI etc) -- Monitoring and Management. (Rate Card based)
    xiv. Hyperconverged Infrastructure (HCI) -- Monitoring and Management. (Rate Card based)
2. Server OS Management Services for all types of hosted Operating systems like Solaris, Windows, ESXI/VMware, Linux, Containerized RHEL OCP/OKE, Unix, Customized OS, Ubuntu and other OS variants etc
3. Database Management services for all types of deployed Databases like ORACLE, MS-SQL, PostgreSQL, Sybase, Redis, MY-SQL, IBM-DB2, etc
4. Middleware management services for all types of Middlewares like Weblogic, OHS, IBM WAS, WebSphere, MQ, JBOSS, Apache Tomcat, JDBC (Java Database Connectivity) and ODBC (Open Database Connectivity), Apache, MQ, HTTP, HTTPs, Rabbit and Apache Kafka. etc.
5. Patching / Security Vulnerability Compliance Management services (VAPT Closure & Patch Management services) on hardware, OS, DB, Middleware and other Datacentre components like HSMs and Load Balancers etc.
6. Upgrades and installations of EOSL Servers, OS, DB etc
7. Management of Underlying Infra for Application Performance Management, Capacity Management tools like OEM, and ITSM tool, etc.
8. Data Centre, Disaster Recovery Centre and Near DR (NLS) operations.
9. DC-DR Drills including readiness of Setups at all sites to meet the defined RTO/RPOs.
10. Management & Monitoring of Bank's License management tool- Flexnet.

11. Management & Monitoring of Bank's Capacity management tool like Oracle Enterprise Management (OEM).
12. Management & Monitoring of Bank's Enterprise Management System for monitoring ITSM & APM.24x7x365 On-site Support Services for management, monitoring and administration of DC, DR, NLS.
13. Helpdesk Support 24x7x365 days to support the Bank for all above infrastructure Management, Monitoring, Administration & Operational issues.
14. Coordination with vendors for various application services which are currently directly managed by Bank's Datacentre teams.
15. Conducting periodic inspection in cages for the servers & assets for proactive maintenance and extending hardware lifespan.
    i. Monitor Physical Hardware in the cage area for any anomaly, malfunctioning and amber. Intimate Bank Team for logging case with the respective Vendors/OEMs for replacement of downgraded assets, parts and passives.
    ii. Capturing logs as per OEM requirement and raising the SRs or Calls along with requisite logs on OEM portal. Coordinate with the OEM resource till RMA call is resolved.

Note:

- In wake of many Regulatory and Operation requirements, Bank has also embarked on different technological enhancements and may implement any new technology/product or refresh existing product during the contract period. In such a case, Managed Service Provider (MSP) has to maintain, monitor and support the imbibed technology (OS, DB, Middleware, Containerization etc) and IT Infrastructure also in line with the scope already detailed in the RFP.
  An annual growth of 10-15% and an annual decrease of 5% in the setups needs to be factored by the MSP. While projections have been factored, the actual baselines will be reviewed at the time of BAU handover/takeover
  Any infrastructure solution or asset, whether hardware or software, which will be managed by Managed Service Provider (MSP) currently and is refreshed/upgraded due to EOSL or upgrade in Technology/Feature, and is replaced by any new/upgraded hardware/solution or asset, MSP shall need to continue to maintain, monitor and support the new/upgraded/refreshed solution as per the defined scope of work, after handover by the Bank through respective OEM/Partner without any additional cost to the Bank.
- MSP has to acquire the required skillsets for any upgradation in respect of Infrastructure Application, maintenance, integration and support during the contract period whenever requested by the Bank as per requirement.
- Bank may include/exclude any of the application assets/hardware of the modules under scope at its own discretion by informing the same to MSP in advance. Any new inclusion of the application/assets will be discussed by the Bank and MSP, and taken over by MSP after proper handholding & KT by the Bank team (if required).

Bank has also embarked on different technological enhancements including Cloud adoption, Data Lake, Hyper converged Infrastructure (HCI), Digital Architecture etc. and hence, Bank may include/change the scope of services mentioned in the SOW in a phased manner with a 30 day notice period at any time during the contract period.

For broader understanding, the scope of work of the DC-NLS-DR Monitoring & Management services engagement (24X7 basis) against each module is divided into sections as summarized in table. 1 below:

The major areas of support which will be covered as part of the scope are given below:

S.N.	Sections	Sub-Sections	Activities	Service Management
4.1	**BAU Activities**	Server Management	Monitoring Administration VM Monitoring & Management (Patching, Hardening, Firmware Upgrade) Email & AD Management	Availability Management Configuration Management Performance Management Incident Resolution ITSM & APM Flexnet Containerized RHEL OCP/OKE Oracle Enterprise Management (OEM)

		Database Management	Monitoring Administration Management Patching, Upgrade Installation & Deployment	Change Fulfilment Service requests/Problem Call Resolution User and accounting Management Capacity planning & Augmentation DR & BCP Compliance and Audit SLA Management Upgradation and Migration Reporting & Documentation Run Books & SOP creation Knowledge Base Documentation
		Middleware Management	Monitoring Administration Configuration Patching, Upgrade Installation & Deployment	
		HSM & Load Balancer Management	Monitoring Administration	
		Storage & Backup Management	Monitoring Allocation Configuration Administration Backup & Restore	
		DR Management (BCP)	DR setup, sync, monitoring, failover drills	
		Upgradations & Migration Activities		
		Governance & Escalation Management		
		Onsite Personnel Deployment & Compliance		
		Compliance & Security		
		Incident, Problem and Change Fulfilment		
		Cage Area Monitoring & Coordination for RMA		
		Asset & Configuration Management		
		Vendor & Third-Party Coordination		
		Helpdesk Support 24x7x365		
		Risk & Audit Reporting		
		Exit & Knowledge Transfer		
4.3.	**Rate Card Based Scope of Work**	Scope of work w.r.t Migration of setups from Cloud/Hosted Models to On-Prem Infrastructure or vice versa		
		Scope of work w.r.t Management of Hyper-Converged Infrastructure.		

Table 1: Summary of Scope of work

5. Detailed Scope of Work

5.1. Server Management (OS Management & Virtualization Management)

5.1.1. Monitoring

- Perform monitoring of all the servers in the Customer's data centres and Near Line Site, for the following parameters by polling the servers at pre-defined intervals:
  - Availability of the server
  - File System / Partition Utilization as applicable
  - Virtualization
  - Memory utilization
  - Processor utilization
- Managing Disk space network Utilization related to server
  - Monitor CPU, Kernel, Disk, Memory, I/O and all other important System parameters
- Monitor critical services related to operating systems and performance tuning.

- Configuring monitoring and alerting systems, including periodic event log analysis and investigation of recurring incidents to maintain server integrity
- Verify system/storage logs and periodically clean up log files/mount points
- Inform bank of any impending problems which can potentially lead to system crash or performance degradation and preparing Major Incident Reports (MIR) along with RCA for significant incidents.
- Log tickets in the helpdesk tool for valid alerts
- Incident / Request Fulfilment / Change management
- Conducting periodic audits in cages for the servers & assets for proactive maintenance and extending hardware lifespan.
    i. Monitor Physical Hardware in the cage area for any anomaly, malfunctioning and amber. Intimate Bank Team for logging case with the respective Vendors/OEMs for replacement of failed drives and parts.
    ii. Capturing logs as per OEM requirement and raising the SRs or Calls along with requisite logs on OEM portal. Coordinate with the OEM resource till RMA call is resolved.

5.1.2. Server Administration

- Create, modify and delete user groups, users and user properties
- Managing network shares, terminal services, cluster services, and file servers, including creation, modification, deletion, and reconfiguration as needed.
- Assign user access rights as per policies defined and agreed upon with the Customer, including account policies like password length, age, and administrator/supervisor password restriction
- Assign space usage restrictions and manage disk space, volume groups, and server resource utilization (disk, processor and network etc).
- Configure and maintain print servers, print queues, terminal services, cluster services, and file servers.
- Maintain and administer DNS, DHCP (including scopes and reservations), NFS, NIS, DFS roots, group policy, and file system mounts.
- Restore server operating system in the event of a crash using backup tools as provided by customer or proposed as part of solution
- Resolve server problems like system hang, hard disk crash, with OEM support wherever required
- Create new file systems and correct file system inconsistencies as and when required
- Installation, configuration, and administration of file systems, volume managers, including LVM administration.
- Configure the print servers, terminal services, cluster services, and file servers.
- Perform periodic system performance tuning as per Customer's policy
- Perform periodic schedule maintenance activity
- OS & Server Hardening and Patching as and when released by OEM or as per patching cycle. Firmware upgrades for hardware as and when released by OEM.
- Implementation of Audit/VAPT recommendations
- Installation, reinstallation, upgrade, and migration of the operating system as required or due to incidents
- Configuration and administration of OS, Logical partitioning of LVM, and HA configuration. Cluster Administration(HACMP) /Installation/Re-installation
- Backup of Operating System, Vhdx, root backups, BMRs etc.
- Commissioning and de-commissioning of servers
- Server Reinstallation and configuration due to Incident
- Managing server build and provisioning with or without automation tools
- Creation of shell scripts or batch programs to automate certain procedures
- Capacity Management & augmentation with respect to CPU and RAM along with intimation to Bank for any best practices and recommendations.
- Adding servers to the clusters (Active-Active & Active-Passive Clusters) and configure, monitor and maintain the cluster functioning as per requirement.
- Migration of server VMs or application Servers/VMs hosted on EOSL hardware to new Hardware with same or upgraded compute configuration and with or without OS, DB and Middleware Upgrade.
- Co-ordinate with SSL Certificate vendor/Bank for issuing and deployment of SSL certificates and further timely deployment of the same
- Carry out DC-DR Drills to meet Regulatory Compliances within defined RTO and RPO times including Server pre-checks and monitoring for smooth switchover & switchback.
- Timely closure of the identified OS/ database/middleware vulnerabilities.
- Implements and enforces security/baseline for all OS as per the hardening document of the Bank

- Password management of super users (e.g., root/support) and defining account policies, including password length, age, and administrator/supervisor password restrictions
- Schedule and execute cron jobs and fine tune same under Bank's intimation and approval.
- Creation of shell scripts or batch programs to automate certain procedures
- Patch Management (Update / Preview / Rollback)
- Firmware Management [Upgrade/Downgrade] of HCI/servers/appliances/storages /switches.
- Perform periodic schedule maintenance activity
- Server Snapshot management
- Implement and manage Linux messaging and security solutions to ensure secure communication and compliance.
- Monitor and manage console access to servers, ensuring secure and controlled access.
- Configure and manage Logical Partitioning (LPAR) and Hard Partitioning (HPAR) for optimal server performance.
- Maintain trusted execution environments for file integrity checks and malware protection.
- Configure encrypted file systems to protect sensitive data as per security standards.
- Administer IBM Hardware Management Console (HMC) for efficient server hardware management.
- Perform trend analysis on historical performance data for capacity planning and forecasting.
- Conduct regular vulnerability scanning of all servers and VMs in addition to patching.
- Monitor and alert on the health of hardware components on physical servers and virtualization hosts (e.g., fans, power supplies, temperature, disks).
- Antivirus/antimalware updates and endpoint protection management.
- Antivirus/antimalware installation, updates, and monitoring.
- Recommendations for hardware upgrades, consolidation, or virtualization.
- Customization of OS builds for specific workloads.

5.1.3. VM Monitoring

- Monitoring Virtualization Host servers for availability
- Monitoring Virtual Machines hosted on the Virtualization host for availability
- Basic VM provisioning and de-provisioning tasks
- Managing hypervisor configurations (VMware, Hyper-V, KVM etc.)
- VM Cluster Functioning, Monitoring and Management egs: HACMP
- Optimizing resource allocation (CPU, RAM, storage)
- Monitoring of performance metrics like CPU, Memory of Virtualization host server

5.1.4. VM Management

- Creating, modifying, deleting Virtual Machines (VMs)
- CPU & Memory resource allocation to VM
- Troubleshooting issues with Virtualization Host servers & VM
- Migration of VM from one host to another or from One Base machine to another.
- Data store migration
- Template creation & cloning of VMs along with migration onto other hardware with same or upgraded compute configuration.
- Hardware /Virtualization OEM Vendor co-ordination
- VM performance tuning
- Virtualization Host patch management
- P2V , Physical to VM conversion or vice versa
- Upgradation of virtualized software
- Advanced troubleshooting of hypervisor kernel and networking issues
- Integrating cloud-based virtualization (Azure, AWS, GCP)
- Environment provisioning and configuration
- VM Snapshot management

*5.1.5. Open Shift Cluster Containerization Support (**This is regarding the management of the underlying infrastructure environment exclusive of platform configuration of the Kubernetes engine)*

- Resource Allocation: Allocate proper CPU/Memory request C Limits for each POD & also defining the Resource quota at Namespace level. Resolving issues related to insufficient resources, such as CPU, memory, or storage within the OpenShift environment. Configure, modify & set project quotas and limit ranges.
- Cluster Health Monitoring: Check cluster utilization and share reports to Bank when needed. Identifying and resolving performance degradation or resource bottlenecks in OpenShift clusters. Resolve issues

with pods like crash loop backoff, image pull back and other errors. Forecast capacity growth requirements and intimate bank for augmentation and handle capacity increase. Perform health checks of the cluster and fix issues based on observations.

- Logs and Metrics Analysis: Collecting and analysing logs from OpenShift and Kubernetes components to diagnose issues or performance problems. Retention of various logs (i.e. App Logs, Audit Logs, Infra Logs).
- Configuration Tuning: Adjusting configuration settings for optimal performance (e.g., tuning resource requests and limits, configuring storage classes). Troubleshooting problems related to pod creation, deployments and scaling.
- Cluster Settings & Troubleshooting: Troubleshoot issues with master/worker/infra/bastion nodes, maintenance and scale-out tasks. Assisting in fine-tuning settings, adjusting pod deployments, storage configurations, and service accounts.
- Issues: Troubleshooting connectivity issues, including problems with ingress controllers, or DNS.
- Handling Patch Updates: Installing minor patches or updates to the OpenShift platform and container runtimes. Deployment of latest OS patches on Bastion, Master, Infra, Worker, and Mirror Registry servers.
- Version Upgrades Assistance: Upgrading to newer OpenShift versions and fixing issues post-upgrade (if any).
- Root Cause Analysis: Analysing complex, intermittent, or critical issues that affect the overall system's availability or performance. Identifying the underlying causes of complex problems, such as persistent failures, systemic issues in application workloads, or systemic network problems in the OpenShift platform.
- Upstream Bug Fixes: Identifying, diagnosing, and working with Red Hat's engineering team or the upstream community to fix critical bugs or vulnerabilities in OpenShift or Kubernetes components.
- Custom Kernel or Software Debugging: Resolving issues that involve debugging, such as kernel panics, performance regressions, or complex multi-node failures that affect the availability of the entire OpenShift cluster.
- Users and User Roles: Create, modify and delete projects/roles. Assign project specific roles to users/groups. Add/remove users and assign roles to group/users. Service account mgmt., role creation and assigning roles.
- Authentication/Authorization Problems: Highlight & Resolve issues related to Role-Based Access Control (RBAC), such as improper permissions or security policies. Troubleshooting user authentication issues and resolving problems with integrated identity providers.
- DR Drills; DC to DR switchover switchback activities with respect to OpenShift cluster. Production cutover and rollout readiness from OCP.

5.1.6. *Email Management:* ***This includes end-to-end management and operation of Microsoft Based Hybrid Mail Messaging setup with the scope mentioned below but not limited:***

- Daily tracker on the Creation / Deletion of the Users
- Daily monitoring of MS-Exchange services health alerts and on time reporting to CSB team and to OEM support team for issues
- Respond to users' emails in stipulated time for acknowledgement
- Management of MS-Exchange Users (Creation/deletion/Unblock/block/Password reset) and Exchange servers (Mailbox Servers, Mail Routing servers etc.)
- Daily operations (Content filtering/ attachment restrictions etc.)
- End user Outlook profile creation & troubleshooting
- Write and maintain documentation for procedures, processes, SOP's, run book, knowledge sharing and configurations
- Provide ITSM support by handling all types of tickets, including Incident / Request Fulfillment / Change management
- Reports should be submitted as per bank's discretion
    - Monthly Mailbox Creation / Deletion
    - Health Status report of Exchange Servers
- MS-Exchange on premises server administration, monitoring and management
- OS patching related required support
- Management of End to end, DR drill of MS-Exchange
- Set up MS-Exchange standard and best practices in line to the bank requirement
- Troubleshooting of daily operational issues on Mailing, connectivity and mobility etc

- Closing of compliance and audit points related to email system
- Maintain a high level of availability for all MS-Exchange services
- Collaborate with other IT teams to troubleshoot and resolve technical issues
- Assistance during any production issue related to MS-Exchange and its components
- Creation and administration of MS-Exchange rules & policies
- Administration of bulk email solution (name of the bulk email platform)
- Configure and manage calendar free/busy sharing to facilitate seamless scheduling
- Configuration of TLS/SSL encryption for secure mail communication.
- Provide advanced troubleshooting for front-end/back-end configurations, including OWA, RPC/HTTP, and ActiveSync
- Implement and enforce MS-Exchange standard configurations and best practices in alignment with the bank's security and compliance requirements
- Lead the implementation, rollout, and administration of MS-Exchange services, ensuring high availability and security
- Manage and optimize hybrid MS-Exchange environments, integrating on-premises and cloud-based identity solutions
- Oversee compliance and protection management like retention policies, filters, DLP, quarantine
- Fine tuning security parameters of all workloads of MS-Exchange
- Implementation and decommissioning of Exchange servers
- Suggest new improvements in existing setup
- Compliance Management
- Journal rules/databases/mail boxes/end user request Management.
- Exchange Database / DAG management
- User mail box issues.
- Public Folders/ users Management.
- Managing different rules on Exchange.
- Integration with other Devices/ Applications
- Distribution Groups creation, member/user and Access Management.

5.1.7. *Active Directory Management:* ***This includes end-to-end management and operation of Microsoft Based AD & allied Structure (DNS etc) setup with the scope mentioned below but not limited:***

- Manage pre-created directory structures
- Manage domains & domain objects
- Monitoring & Management of Active Directory Replication
- Monitoring and troubleshooting of network connectivity of all servers
- Implement and Manage Enterprise Group Policies
- Modification in directory structure if required
- Enhancing AD security with conditional access and zero-trust models
- Designing AD architecture and domain forest strategies
- Implementing identity federation and hybrid AD solutions
- Integrating AD with cloud-based identity providers (Azure AD, Okta)
- LDAP for centralizing user/group management
- Perform backup and recovery of AD servers and AD objects
- Perform the addition of servers to the domain as per defined policies and procedures.
- Identify and resolve domain-related issues to ensure seamless operation and connectivity.
- Update and manage DNS records to maintain accurate and efficient domain name resolution.
- Configure and maintain DHCP settings to ensure proper IP address allocation and network functionality.
- Administer Active Directory (AD) sites and services to optimize replication and network performance.
- Perform monitoring and analysis of server logs to identify and address potential issues proactively.
- Under Federation Services Management: ADFS (End –to end maintenance of ADFS servers/users/access management.)
- Administration of FSMO roles and AD schema updates.
- Enforcement of password policies, account lockout policies, and multi-factor authentication (MFA) integration.
- Regular optimization of AD replication and Exchange database performance.
- Capacity planning for mailbox storage, AD object growth, and database sizes.
- Recommendations for upgrades and performance tuning.

5.2. Database Management

5.2.1. Database Monitoring

- Perform monitoring of standard critical parameters for the database (monitoring of which is supported as per the deployed DB license) during the service window agreed in this SOW such as:
  - Table spaces & database objects and segments.
  - Mount points of logs and data files
  - Availability of background processes
  - Buffer cache utilization
  - Highlighting Resource intensive queries through AWR reports along with their impact & RCAs
  - Fragmentation of table spaces indexes
  - Memory, I/O, CPU utilization for the RDBMSs monitored at OS Level
  - Machine Availability

- ***DB-Application Parameters:***
  JVM Heap utilization
  JVM Garbage Collection Time
  Sync connection
  Total Defunct Processes
  Overall Application Average Response Time

- ***DB Server Parameters:***
  CPU Usage
  Disk free space
  DiskSpace Utilization
  Swap Usage
  Uniser Monitoring
  Load Average
  Analytics agent

- ***Database Parameters:***
  Memory Utilization
  CPU Utilization
  Average Active Connections
  Database Warning
  Queues and Waits
  IO Requests
  Active and Defunct or Lock Sessions
  Invalid Object Count
  Active & Archive Files Size Check
  User Account Lock
  Long running query

- ***DB Log Parameters:***
  Alert logs for errors
  Database backup Logs
  Transaction Logs
  System Errors
  Instrumentation Logs & Errors

- Monitor system performance and provide performance data to Customer as per requirement.
- DC and DR sync verification, either manually or through the customer provided tool if sync check is automated.
- Monitoring & taking corrective actions (in coordination with Bank Team) for Replication technologies like Oracle Data Guard (ODG), Active Data Guard (ADG), Storage Replication, Synchronous & Asynchronous Replication, SQL Server Replication functioning and related parameters.

5.2.2. Database Administration

- Create, modify and delete database and database objects

- Create, modify and delete users and properties
- Create, modify and delete maintenance jobs
- Perform periodic database performance tuning as per the documented procedures
- Perform periodic house-keeping of Database
- Perform orderly start-up and shutdown of database services
- Add, modify and delete permissions to database objects and troubleshoot user logins
- Cache Optimization
- Rectify database configuration problems
- Based on Customer's policy provided during transition:
  - Perform regular defragmentation, truncation & partitioning activities for better space management and performance tuning.
  - Grant and revoke database access to users
  - Execution of scheduled database jobs
- Database performance tuning and response monitoring
- Creation of shell scripts or batch programs to automate certain procedures
- Carrying DC- DR drills as per the SOP or through Workflow tools (as per availability).
- Upgradation of databases to higher stable versions.
- Implementation and configuration of the replication setup for DR and near site, monitor the sync status (Synchronous & Asynchronous), Storage Replication.
- Housekeeping on DR server & cleaning up of Archive logs and Alert logs/transaction logs
- Assisting in backup and restoration tasks as per Bank's requirement.
- Coordination with the OEM Vendors for Product Bugs and Support
- Install Database Software along with Database Hardening / Database Patching.
- DB Hardening and Patching as and when released by OEM or as per patching cycle.
- Microcode upgrades for DB hardware as and when released by OEM.
- Troubleshooting deep-level database engine issues
- Working with application teams to improve database efficiency
- Cluster Management (HACMP)
- Architecting high-availability (HA) and disaster recovery solutions
- Re-build DC and/or DR instance from available backup in case of crash & Restoring OS from MKSYS backup.
- Troubleshoot and resolve RAC (*2 node or 3 node*) issues and partitioning-related issues to ensure database availability and performance.
- Perform import, export, and archival of databases to support data migration and backup processes.
- Execute and manage various types of database backups for all applications to ensure data integrity and recovery.
- Perform database native backup operations, including RMAN, to maintain data protection and recovery readiness.
- Ensure Database and Application backups are in place as per Bank's policy/requirement and resolve database crashes and perform rebuilds as required to restore database functionality.
- Resolve database backup issues (if any) and perform rebuilds as required to restore database functionality.
- Troubleshoot and resolve unexpected database instance hangs or terminations to ensure continuous operation.
- Conduct session-level audits to monitor and ensure compliance with database access and usage policies.

5.3. Middleware

5.3.1. Proactive Monitoring

- Monitor web server and middleware server availability
- Monitor availability of the services deployed in the web server and middleware servers
- Monitor alert notifications, check for impending problems, triggering appropriate actions
- Monitor client connection status
- Monitor threshold values for key parameters such as memory usage, file system usage
- Performance tuning and troubleshooting middleware failures
- Load/stress testing and tuning of middleware configurations.
- Optimize performance for application-middleware-database integration.
- Assisting in application deployment following runbook procedures

- Managing user access and authentication for middleware services
- Managing SSL certificates for middleware components
- Implementing advanced security configurations and encryption techniques
- Monitor middleware resource use such as connection pooling
- Monitor CPU, memory, heap, garbage collection, thread pools, and connection pools.
- Audit and monitor middleware logs for suspicious activity.

5.3.2. Administration

- Perform start up and shutdown of web/middleware server instances
- Provide support for known errors and problems
- Escalate calls as per the escalation matrix
- Coordinate with escalation team to close calls
- Update knowledge base on closure of a call
- Coordinating with application and security teams for compliance adherence
- Troubleshooting deep-level middleware performance and integration issues
- Log calls based on the monitoring alerts
- Raising change requests related to Middleware Services
- Manage clustering, load balancing, and failover configurations.
- Backup all middleware configurations, security certificates, and related artifacts.
- Maintain up-to-date configuration documentation.

5.3.3. Installation and Configuration

- Perform pre-Installation tasks during crash recovery process and for new installations
- Perform web server and middleware server configuration (e.g., WebLogic, JBoss, Tomcat, WebSphere) during a crash recovery process and for new installations
- Deploying patches and upgrades for middleware applications
- Configuring and maintaining middleware services (e.g., WebLogic, Tomcat, JBoss, MQ environment variables, JVM parameters, memory settings.)
- Implementing automation for deployments and configurations
- Architecting middleware solutions for high availability and scalability
- Designing and optimizing enterprise middleware infrastructure
- Version and build management for middleware components.
- Implement security hardening measures for all middleware platforms.

5.4. HSM & Load Balancer

5.4.1. HSM& Load Balancer Administration and Management

- Installation-reinstallation, configuration and management of Load balancers.
- Troubleshooting the end to end connectivity and flow between the HSM & Load balancer devices and backend servers
- Load Balancer Management (creation of Virtual Service, mapping the servers, Firmware upgrade, user management, etc)
- Upgradation of the load balancer devices, firmware, patches (as and when released by OEM), softwares and OS as per the organization policies
- Installation-reinstallation, configuration and management of HSMs (Network based and PCI based as applicable).
- HSM management, administration and monitoring of HSM hardware health, network interfaces and connectivity.
- Firmware upgradation, patch management and OEM recommended updates in HSM devices.
- Monitoring of HSM performance and security logs.
- RCA for HSM & Load Balancer related incidents.
- Periodic secure backup of key material and HSM configuration (offline and tamper-proof).
- Testing of DR Site HSMs and Load Balancers and ensuring synchronization with primary site.
- OEM coordination for hardware replacement and bug fixes.
- Support for DR drills as per the drill calendar or as and when needed
- Timely closure of the identified vulnerabilities in coordination with the OEM
- Proactive monitoring and escalation of incidents
- Proactively monitor Load Balancer device health status to detect and report issues
- Implement changes, including creation or deletion of VADCs and connectivity setup
- Support Switchover and Switchback processes at the Data Centre

- Handle complex escalations, including system-wide outages and critical incidents
- Provide expertise on change management, ensuring minimal downtime during major updates
- Load balancing during EOD and SOD job
- Monitoring of CPU, memory, throughput, SSL TPS (transactions per second), session counts, and connection tables.
- Application-level performance monitoring (L4 and L7) to detect latency, packet drops, and service degradation.
- Allocation of virtual network interfaces, IP addresses, and VLAN bindings.
- Resource assignment (CPU, memory, throughput limits) per vADC to ensure optimal load distribution.
- Configuration and optimization of supported protocols:
- Configuration of appropriate load balancing methods, including but not limited to:
- Implementation of persistence/sticky sessions policies (source IP, cookie, SSL session ID, etc.).
- URL rewriting and redirection rules.
- Compression, caching, and connection multiplexing for performance optimization.
- SSL bridging, SSL pass-through, and mutual TLS authentication configuration.
- Implementation of access control lists (ACLs), IP restrictions, and rate-limiting policies.
- TLS cipher suite optimization to meet industry standards (e.g., disabling weak ciphers).
- Integration with Web Application Firewall (WAF) and other security tools where required.
- Scheduled configuration backups of all load balancers and vADCs/tenants.
- Verification of backup integrity and periodic restoration testing.
- Version control of configuration changes with rollback capabilities.

5.5. Storage & Backup Monitoring

5.5.1. Storage Administration Tasks

- Monitor storage utilization, performance metrics, and capacity trends to ensure optimal resource allocation.
- Implement 24×7 monitoring for all storage and backup systems using Bank-approved tools.
- Configure alerts for threshold breaches (capacity, performance, job failures, hardware errors) and ensure timely incident resolution.
- Maintain real-time dashboards for Bank's visibility into storage and backup health.
- Maintain thresholds for proactive scaling before reaching critical utilization levels.
- Monitoring of the SAN/NAS devices for availability as per the service window agreed in this SOW
- Perform storage user administration
- Perform disc quota and rights or permission administration
- Coordinate with the hardware vendor for addition, deletion or modification of RAID configuration
- Add, delete and modify LUN configuration
- Perform physical disk management
- Configure, and manage storage and SAN switches
- Configuring and managing storage arrays (SAN/NAS)
- Configure the SAN Switch for Host Mapping
- Perform incident based troubleshooting
- Create and map Logical Unit Numbers (LUN) and volumes to different servers based on the inputs provided by the Customer
- Manage disk space on LUN
- Managing snapshots and replication configurations
- Hardware, software and firmware upgrades as and when released by OEM
- Creation of Storage Pools and Volume Groups
- Reporting to Bank in case of any difference in replication and resolve the same in coordination with OEM & Network Team
- Managing complex storage migrations and integrations
- Performance tuning and troubleshooting IOPS issues
- Advanced performance tuning for high-demand applications
- Replication Management [Creation/Modification/Deletion/Monitoring/Synchronization of storage replication]
- Troubleshooting vendor-specific storage hardware/software issues
- Configure and allocate the required storage capacity based on inputs provided by Customer
- LVM Administration

- Manage and maintain storage switches and NetApp filers to ensure optimal storage performance and availability.
- Configure and administer Storage Area Network (SAN) environments to support data storage and access requirements.
- Perform administration and management of file systems, including JFS and JFS2, to ensure efficient storage utilization.
- Implement device masking, port settings, and fabric zoning to ensure secure and efficient storage connectivity.
- Administer, configure, and maintain all SAN, NAS, and object storage systems, including disk arrays, storage switches, and related components at both DC and DR sites.
- Implement storage tiering policies for optimal cost–performance balance.
- Maintain high-availability configurations and perform failover testing for storage systems.
- Perform quarterly capacity forecasting for storage and backup infrastructure.
- Recommend capacity expansion, storage reallocation, and archival strategies to optimize performance and costs.
- Identify underutilized storage resources and reclaim them for productive use.

5.5.2. Backup and Restore Management

- Modification to backup policy in consultation with the Customer and adhere to the policy
- Modify the backup retention policy in consultation with customer
- Provide routine backup and recovery of data with respect to the IT Infrastructure
- Periodically monitor the log generated by the backup tool and take appropriate actions
- Monitor the performance of scheduled backups, schedule testing of backups as per policy agreed with customer during transition and enable the adherence to related retention policies
- Review backup logs to verify successful completion of backup
- Notify to customer team any backup failures through automated report, ticket etc
- Perform restoration drill as per the schedule agreed with customer during transition and sign off within the limit of available hardware in scope
- Management and administration of the Backup software
- Verify storage logs and periodically clean up log files
- Restricting backup window as per customer specific guidelines
- Scheduling and monitoring of OS-level backups.
- Restoration testing for OS recovery at regular intervals.
- Configuration for OS image backups and bare-metal recovery.
- Validate backup integrity through periodic test restores.
- Configure, monitor, and administer all enterprise backup systems...
- Maintain backup schedules, policies, and retention plans...
- Manage offsite backup copies and coordinate secure transport...
- Implement data encryption for backups based on the features of the backup solution.
- Execution of daily, weekly, and incremental Exchange database backups.
- Verification of backup integrity through periodic test restores.

5.6. DR Management

- DR drills will be conducted in scope infrastructure with pre-identified locations and business users participating in a single drill.
- Vendor will support the customer in performing switchover and switchback activities as per the defined scope.
- Configuration at the Primary Data Center (DC) is to be done by the client unless it is also under the managed scope.
- The ISP engaged by the customer will be responsible for ISP-level failover and any changes required for failover to the DR site and back during the DR drill exercise.
- The customer must enable business users' systems with the required configuration to access applications from the DR site.
- The customer will initiate the DR drill and execute the Business Continuity Plan (BCP).
- The customer must provide a minimum of 30 days' advance notice to initiate scheduled DR drills.
- DR drill pre-checks must be conducted.
- Primary and DR replication must be monitored.

- A comprehensive Disaster Recovery Plan (DRP) must be developed, maintained, and updated in alignment with the Bank's BCP.
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be defined and documented for all critical systems and services.
- An updated Application–System–Infrastructure mapping must be maintained to ensure DR readiness.
- All production workloads must be validated to have replication or backup mechanisms to the DR site.
- Drills must include performance testing of applications post-switch and validation of data integrity after failover and reverse failover.
- Detailed drill reports must be documented and submitted.
- Coordination with all stakeholders is required to ensure rapid service restoration.
- Monthly DR readiness reports must be provided.
- Version-controlled DRP documents must be maintained.
- Zero data loss beyond the defined RPO must be ensured in all DR events, whether drills or real incidents.

5.7. Other Activities:

5.7.1. Upgradation & Migration Activities:

In addition to monitoring, administration and management of DC components, the MSP/Service Provider shall be responsible for carrying out all required upgradation, migration (EOL/EOS assets) [10-15% for Y1, 5-10% for Y2 and Y3] (Pls note, While projections have been factored, the actual baselines will be reviewed at the time of BAU handover/takeover) in the Bank's Data Centre (DC), Disaster Recovery (DR) Site, and Near DR/NLS (if applicable) in a structured, secure, and SLA-bound manner. The activities will include but not be limited to the following:

- Active support for ongoing projects like upgradation / migration of systems to latest supported platforms.
- End-to-End Upgrading end of life Servers, OS, DB and middleware systems.
- Validate application compatibility post-patch/upgrade/installation/re-installation.
- Assessment of existing servers, storage, network devices, and security appliances for compatibility with latest versions of firmware, OS, and applications.
- Ensuring application compatibility post-upgrade/post-installation through pre- and post-implementation testing.
- Testing, validation, and acceptance sign-off from Bank's application teams before production cutover.
- Migration of databases to new hardware or cloud/hybrid environments, as required.
- Detailed migration plan with timelines, dependencies, and rollback strategies.
- Functional, integration, performance, and security testing after each upgrade/migration.

Please note, Migrations shall be included in the BAU scope for the components that cannot be upgraded due to technical constraints, OEM recommendations and/or hosting constraints and in all cases need to be migrated onto new hardware. Additionally, End-of-Life (EOL) and End-of-Support (EOS) upgrades shall also be the part of the upgrade process & BAU Activities. If an application requires a database (DB) or operating system (OS) upgrade, it shall be carried out as part of BAU activities.

5.7.2. Governance & Escalation Management

a. Domain Lead (Service Manager)
   - The bidder shall designate a DC, DR, NLS Lead and a Domain Lead (Service Manager) for all workstreams. The DC Lead & Service Managers will act as the single point of contact for all service/incident/problem/change-related escalations and must be accessible 24x7 via telephone, email, and web assistance. They will provide support to J&K Users and the CSD team, assisting with problem resolution, addressing concerns and queries, and handling service requests.
   - The bidder should provide the contact list of DC, DR, NLS leads & domain leads who shall attend to domain-level escalations.
   - The Bidder shall ensure that an escalation matrix is in place, detailing response timelines and responsible personnel for each escalation level.

b. Governance Framework
   - Establish a joint governance structure between the Bank and the Service Provider for overseeing Data Centre operations, including a steering committee, operational committee, and working groups.

- Prepare and maintain Service Delivery Governance Documents, including governance charter, RACI matrix, and reporting templates.
- Conduct periodic service review meetings at different levels:
  - Executive Level – Quarterly review of service performance, risks, and strategic initiatives.
  - Operational Level – Monthly review of SLA compliance, incidents, changes, and improvement plans.
  - Technical Level – Weekly review of operational issues, tickets, and planned maintenance activities.
- Ensure that governance meetings are minuted, and action items are tracked to closure within agreed timelines.
- Submit governance reports summarizing SLA performance, incident trends, capacity utilization, risk register, and improvement recommendations.
- The MSP shall conduct monthly governance meetings with J&K Bank stakeholders to review SLAs, discuss major incidents, major changes, RCA reports, and improvement plans.

c. Escalation Management
- Implement a multi-level escalation matrix covering functional, technical, and managerial contacts from both the Bank and the Service Provider.
- Ensure clear definition of escalation triggers such as breach of SLA, prolonged incidents, repeated service failures, or unresolved service requests.
- Maintain round-the-clock availability of escalation contacts for critical and high-severity incidents.
- Escalations must follow a time-bound process:
  - Level 1 – Frontline resolution within defined SLA timelines.
  - Level 2 – Functional/technical expert involvement within 30–60 minutes of SLA breach or as per incident priority.
  - Level 3 – Senior management intervention within 1–2 hours for critical issues.
- Ensure proactive escalation to prevent SLA breaches and minimize business impact.

d. Reporting & Communication
- Provide incident escalation reports with details of root cause, resolution, and prevention measures.
- Share monthly escalation dashboards highlighting number of escalations, causes, resolution timelines, and recurrence trends.
- Maintain real-time communication with Bank's NOC/IT teams during escalated incidents.
- Ensure that post-resolution, lessons learned are captured and incorporated into SOPs and preventive measures.

e. Continuous Improvement
- Analyse escalation patterns and recurring issues to identify process gaps and propose corrective actions.
- Recommend automation or process enhancements to reduce escalations.
- Implement service improvement plans (SIPs) with measurable outcomes and agreed timelines.
- Align governance and escalation processes with ITIL best practices and the Bank's internal standards.

5.7.3. Personnel Deployment & Compliance

a. Personnel Deployment & Training
- Deploy adequate number of personnel in line with the Bank's approved manpower plan, covering 24x7x365 operations, including weekends and public holidays. Always maintain minimum staffing levels as agreed with the Bank.
- Ensure that deployed resources cover all the roles and areas as asked for in this RFP.
- OEM-certified specialists for all domains and technologies as asked for in this RFP. Ensure that all personnel have the required technical certifications, skills, and experience for their assigned roles.
- The Bidder shall ensure that all personnel proposed for deployment at the Bank's site are subject to an interview and approval process by the Bank before onboarding.

- If any appointed personnel are deemed unacceptable by the Bank for any reason, the Bidder shall replace them within one week of receiving such intimation, at no additional cost to the Bank.
- The Bidder shall also provide a suitable backup resource in the absence or leave of the onsite resource(s) to ensure continuity of services.
- The Bidder shall ensure that all deployed personnel adhere to J&K Bank's Supplier IS security policies, Acceptable Usage Policy including background verification (BGV), non-disclosure agreements (NDAs), and cybersecurity training.
- Maintain updated personnel records and provide them to the Bank as and when required.
- Provide refresher trainings and upskilling sessions on new technologies, processes, and tools as per project requirements.
- Conduct familiarization sessions on the Bank's IT policies, security guidelines, and operational procedures before personnel begin work.
- Ensure full compliance with applicable labour laws.
- Ensure timely renewal of labour licenses (if applicable).
- Bear all statutory liabilities related to personnel, including wages, benefits, insurance, and any legal claims.

b. Code of Conduct & Discipline
- Ensure that all personnel follow the Bank's workplace conduct guidelines, including dress code, behaviour, and use of facilities.
- Prohibit use of personal devices in restricted areas unless expressly authorized by the Bank.
- Enforce strict adherence to security protocols, including access control, escort policies, and prohibition on unauthorized data access.
- Replace any personnel whose performance, conduct, or behaviour is deemed unsatisfactory by the Bank, within 48 hours of intimation.

c. Continuity & Knowledge Retention
- Maintain low attrition of deployed staff to ensure operational stability.
- Ensure that departing personnel hand over all access rights, passwords, documents, and assets before release.
- Maintain up-to-date handover/takeover documentation to ensure smooth transition between resources.

d. Audit & Verification
- Facilitate periodic audits by the Bank or third-party agencies to verify personnel deployment, skill levels, and statutory compliance.
- Provide access to relevant records, including attendance logs, payroll records, training certificates, and compliance documents.

5.7.4. Compliance & Security

a. Regulatory & Standards Compliance
- All activities under the scope must be carried out directly by the Bidder's personnel. No activity shall be outsourced or sub-contracted to any third party except the one specified and allowed from the bank post due permissions.
- All configurations, changes, and asset updates must comply with J&K Bank's Supplier IS security Policies, cybersecurity guidelines, IT outsourcing policy, and regulatory requirements (e.g., RBI, NPCI and applicable regulatory guidelines).
- Compliance to bank's various ISMS procedures.
- **All regulatory changes**, implementations, customizations & reports (RBI, Central or State Government, semi-government entities, NPCI etc) must be implemented without additional commercials except if the volume is humongous (Significant initiatives that require new resources, architectural changes, or major projects beyond standard operations.) which can be mutually agreed.
- In case of the contract termination due to regulatory changes, bank and bidder can mutually discuss and agree on the further course of action.
- The vendor shall provide all or any specific report requested by the Regulator/ Bank / Bank appointed auditors, within the timelines stipulated in the SLA.
- Ensure that governance and escalation processes are auditable with complete activity logs, escalation records, and meeting minutes.

- Maintain compliance with RBI, CERT-In, and other regulatory requirements related to incident and problem management.
- Facilitate internal and external audits related to governance and escalation management processes.
- Periodically review and incorporate regulatory guidelines (e.g., RBI, ISO 22301, ISO 27031) into the DRP.
- Enforce role-based access controls for storage and backup administration.
- Implement audit trails for all configuration changes and administrative actions.
- Ensure compliance with applicable guidelines (RBI, ISO 27001, ISO 22301, etc.) for data protection and backup retention.
- Support regulatory and internal audits by providing logs, reports, and evidence of compliance.

b. Adherence to Information Security guidelines
- Enforce strong password in line with bank's password policies, multi-factor authentication (MFA), and periodic administrative privilege credential rotation.
- Maintain comprehensive logs of all administrative and privileged activities for at least 1 year or as per Bank's policy.
- Prevent unauthorized physical or logical access to Bank's IT assets.

c. Vulnerability & Patch Management
- Ensure timely remediation of vulnerabilities as pointed out by the bank's information security team or regulator based on severity:
- Critical – within 24 hours
- High – within 3 days
- Medium – within 7 days
- Low – within 14 days
- Apply security patches, firmware updates, and hotfixes in accordance with the Bank's change management process.

d. Data Security & Privacy
- Ensure encryption of data at rest and in transit as per Bank's policy.
- Restrict copying, transfer, or storage of Bank data outside authorized systems.
- Prevent use of personal storage devices in the DC premises.
- Maintain strict confidentiality of all data

e. Compliance Reporting & Audit Support
- Provide monthly compliance status reports to the Bank covering regulatory, security, and policy adherence.
- Maintain all evidence of compliance, including logs, access reports, and audit records, for at least 7 years or as per regulatory requirements.
- Facilitate internal, statutory, and third-party audits by providing required documentation, system access, and personnel support.
- Ensure closure of audit findings within the agreed timelines.

f. Continuous Improvement
- Track industry threats, vulnerabilities, and emerging regulatory requirements, and recommend relevant security enhancements.
- Conduct annual security drills, including disaster recovery, incident response, and breach simulations.
- Provide regular security awareness training for deployed personnel.

5.7.5. Incident, Problem and Change Fulfilment

- Bidder has to follow the Incident management procedure of the bank
- Bidder has to provide RCA for all incidents within 24 hours post incident resolution.
- The Bidder shall maintain a Knowledge Base documenting common incidents, fixes, and best practices to enhance response efficiency.
- The Bidder shall implement automated monitoring & alerting mechanisms to proactively identify issues and reduce incident response time.
- The Bidder shall establish a Service Continuity Plan to ensure smooth operations in case of major outages or infrastructure failures.

- The Bidder shall be responsible for executing approved changes (pertaining to their respective domains), and all change requests must be fulfilled in accordance with the Bank's approved process, ensuring minimal disruption and adherence to security policies.
- The Bidder shall ensure no unauthorized changes are performed and conduct periodic audits to verify compliance with the approved Change Management Process.

5.7.6. Asset & Configuration Management

- The Bidder shall track assets, check quality, and maintain utilization levels, pertaining to their respective domains.
- The Bidder shall coordinate with J&K Bank/third-party vendors and perform configuration management accordingly in assets (Assets in Bidder's scope) to incorporate/add new devices/technology implementations.
- The Bidder shall perform initial asset verification of all hardware/software and establish the Configuration Management Database (CMDB).
- The Bidder shall maintain the asset register and Software Licence Inventory of IT assets inline with Asset Management Procedure and Software Licence Policy of the bank under the scope of DC management, both offline (through Excel) and online (through CMDB), and shall migrate asset records to CMDB as and when needed.
- Maintain version-controlled inventory of all hardware, software, and firmware used in storage and backup infrastructure.
- The Bidder shall update the asset management database to track all moves, additions, changes, and installations. The physical security of assets will be handled by J&K Bank.
- Maintain an up-to-date inventory of all hardware and software assets, including locations, configuration details, serial numbers, asset codes, warranties, and AMC details.
- Track licensed software and applications, movement within sites/between locations, and changes in configurations.
- Ensure the timely decommissioning of EOL/EOS assets in coordination with J&K Bank, providing recommendations for replacements.
- The Bidder shall monitor warranty/AMC details and notify J&K Bank 60 days in advance for contract renewals.
- The Bidder should track software/firmware recommendations from OEMs, coordinate hardware/software/firmware upgrades with OEM/vendors, and update the asset database.
- The Bidder should track End-of-Life (EOL) and End-of-Support (EOS) statuses of devices and inform/advise J&K Bank accordingly.

5.7.7. Vendor & Third-Party Coordination

- The Bidder shall be responsible for coordinating with OEMs/vendors for software updates, security patches, and firmware upgrades, ensuring minimal downtime.
- The selected MSP shall plan, design/re-design, implement, upgrade, operate and optimize all the hardware, software, solutions, assets and applications under scope.
- The MSP shall also be responsible to operationalize a process to ensure alignment with IT infrastructure and application life cycle management process.
- The Bidder shall track and document vendor SLAs, ensuring compliance with service expectations.
- Ensure OEM-certified tools and procedures are followed for all changes.

5.7.8. Risk & Audit Reporting

- The Bidder has to provide a risk register on a monthly basis, along with a mitigation plan in a RACI matrix.
- The Bidder should have implemented Risk Management policies in their organization and should provide Risk Assessment details to the Bank, including BGV of resources assigned to the Bank.
- The Bidder shall establish periodic IT audits, ensuring adherence to J&K Bank's policies and regulatory guidelines.
- Conduct annual risk assessment of the DC and DR sites for vulnerabilities (power, cooling, network, security).

5.7.9. Outcome-Based Delivery Expectations: Expected outcomes may include:

- Reduced Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR) incidents.

- Predictive maintenance and proactive issue resolution.
- Improved system availability and performance.
- Reduction in manual interventions and operational overhead.
- Ability for faster diagnosis through logs correlation, visibility & Infrastructure mapping
- Compliance and audit readiness through automated reporting and controls.
- Capabilities around event correlation, anomaly detection, and root cause analysis.
- Integration with existing ITSM and monitoring tools.

5.7.10. Exit & Knowledge Transfer

a. Exit Management Plan
   - No later than six (6) months prior to contract termination, the Bidder shall conduct comprehensive exit training sessions for the Bank to ensure operational continuity with minimal disruption post-transition. This shall include the complete handover of all relevant documentation, source codes, user guides, and operational insights to the Bank.
   - After each training provided to the Bank, the Bidder shall gather participant feedback surveys and conduct knowledge assessments to measure training effectiveness. Any identified gaps or deficiencies shall be promptly addressed through additional training sessions or corrective measures, ensuring alignment with the Bank's operational requirements.
   - Provide quarterly knowledge transfer sessions to the Bank's IT team on storage and backup health, trends, and optimizations.
   - Failure to conduct the defined training sessions as per the agreed schedule shall constitute a material breach of contract. The Bank reserves the right to take necessary actions/lay the penalty to address non-compliance.

b. Asset & Configuration Handover
   - Provide a comprehensive asset inventory (hardware, software, licenses, configurations, network diagrams) updated to the last day of service.
   - Transfer all original licenses, activation keys, warranty/AMC details, and OEM support contracts related to the Bank's assets.
   - Ensure secure handover of all configuration files, scripts, system parameters, and administrative credentials.
   - Validate with the Bank's technical team that all systems are functioning as per agreed configurations before the final exit.

c. Documentation Transfer
   - Hand over all Standard Operating Procedures (SOPs), design documents, architecture diagrams, process flows, and incident/problem records.
   - Provide detailed records of past upgrades, migrations, changes, and maintenance activities performed during the contract period.
   - Submit an updated knowledge repository containing troubleshooting guides, escalation matrices, and vendor contact details.

d. Knowledge Transfer to Bank/Successor
   - Conduct structured knowledge transfer sessions for the Bank's internal teams or incoming service provider covering:
   - DC/DR infrastructure layout and dependencies
   - System configurations and integrations
   - Operational processes, escalation procedures, and monitoring mechanisms
   - Ongoing incidents or known issues with resolution status
   - Provide hands-on training and shadow-support for a minimum agreed period (e.g., 180 days) post-handover.
   - Ensure all knowledge transfer sessions are documented and acknowledged by the Bank.

e. Personnel Transition
   - Ensure continuity of critical staff during the transition period to avoid knowledge gaps.
   - Replace any personnel leaving during the exit phase with equally skilled resources without impacting service delivery.
   - Facilitate joint working between outgoing and incoming teams for a smooth handover.

f. Data & Access Management
   - Hand over all data, databases, and application repositories in Bank-approved formats.

- Ensure secure deletion/erasure of any Bank data from the Service Provider's devices, systems, or storage media as per Bank policy and provide compliance certificates.
- Revoke all user IDs, passwords, and access privileges to Bank systems, physical premises, and applications held by Service Provider personnel.

g. Compliance & Final Settlement
- Provide an Exit Completion Report signed by both parties confirming successful transfer and acceptance by the Bank.
- Support audit verification of all exit-related activities. Ensure that all obligations, warranties, and service credits are settled before contract closure.

h. Post-Exit Support (If Applicable)
- Provide limited-time post-exit support (remote/onsite) as agreed in the contract, to resolve any unforeseen issues arising from the transition.

6. Rate Card Based Scope of Work

6.1. Scope of work w.r.t Migration of setups from Cloud/Hosted Models to On-Prem Infrastructure or vice versa

6.1.1. Discovery & Assessment

- Assessment and planning of current workloads hosted in cloud/third-party environments.
- Inventory of all applications, databases, dependencies, and services currently in the hosted/cloud environment.
- Performance, capacity, and compliance assessment of target on-premise hardware.
- Risk assessment and mitigation planning.

6.1.2. Migration Planning

- Develop detailed migration strategy and timeline.
- Define migration approach (lift-and-shift, re-platform, re-architecture), timeline, and resource plan.
- Define cutover plans with rollback contingencies.
- Application dependency mapping and downtime planning.
- Identify tooling (e.g., replication tools, database migration tools) and licensing requirements.
- Carry migration of selected applications, databases, and services within defined timelines.

6.1.3. Infrastructure Preparation

- Configure on-premise hardware according to migration needs (compute, storage, network).
- Setup physical or virtual servers, storage, networking components.
- Plan hardware, network, storage, and security architecture aligned with bank standards.
- Install and validate required OS, middleware, and database platforms.
- Ensure compliance with internal security policies and external regulations.
- Incorporate security controls, access management, and compliance requirements (e.g., PCI DSS, GDPR).
- Ensure data backups are in place and DR plans are aligned.

6.1.4. Application and Database Migration

- Perform data replication, migration, and transformation as needed.
- Migrate application code and services to the target infrastructure.
- Transfer databases and data repositories securely and efficiently.
- Configure load balancers, firewalls, DNS, and other networking components.
- Optimize performance tuning and resource allocation post-migration.

6.1.5. Testing and Validation

- Validation, testing, optimization, support and uptime commitment post-migration.
- Functional and regression testing of applications and databases.
- UAT (User Acceptance Testing) support if needed.
- Performance benchmarking and validation against SLAs.
- Minimal disruption to ongoing operations and adherence to security and compliance requirements.

6.1.6. Cutover and Go-Live Support

- Execute final cutover to on-premise infrastructure.
- Move applications ensuring minimal downtime, performing necessary configurations.
- Monitor system performance and availability.
- Provide proper support and uptime like other applications post-migration.

6.1.7. Documentation & Knowledge Transfer

- Provide migration runbooks, configuration documentation, and updated infrastructure diagrams.
- Conduct knowledge transfer sessions for internal IT and operations teams.
- Decommissioning:
- Safely decommission cloud/hosted resources if applicable.
- Ensure all migration activities adhere to banking and regulatory standards.
- Implement necessary security controls to protect sensitive data during and after migration.
- Provide incident, change, and performance reports monthly.
- Submit daily, weekly, and monthly reports covering storage utilization, backup success/failure statistics, restore test results, and SLA compliance.
- Maintain updated configuration documents, architecture diagrams, and SOPs for all storage and backup components.

6.1.8. Project Risk Management

- Identification of various project risks , Complex requirements & integrations can lead to project delays
- Risk of data loss or corruption during implementation
- Data breaches, unauthorised access
- Development of controls & risk mitigation strategies

6.2. Hyperconverged Infrastructure configuration, maintenance and support

6.2.1. Maintenance Tasks:

- System Updates and Patching: Coordinating with the HCI Vendor/team for regularly applying software updates for the HCI platform, including firmware and drivers, and installing security patches to address vulnerabilities are critical for maintaining system health and security.
- Monitoring and Performance Optimization: Monitoring key performance metrics like CPU, memory, disk usage, and network traffic, along with capacity planning to identify and address bottlenecks, ensure optimal resource utilization, and forecast future needs.
- Hardware Maintenance: Inspecting components for wear and tear to ensure proper replacing failed drives, and conducting periodic audits for proactive maintenance.
- Documentation and Reporting: Maintaining detailed records of all maintenance activities, hardware changes, and upgrades is essential for troubleshooting, planning future upgrades, and ensuring compliance.

6.2.2. Support Tasks:

- Troubleshooting and Problem Diagnosis: Addressing issues related to hardware failures, software conflicts, performance degradation, and connectivity problems, often involving the use of diagnostic tools, log analysis, and vendor-specific troubleshooting guidance.
- Technical Support Engagement: Collaborating with vendors and partners for comprehensive technical and remediation support, including resolving software and hardware issues, managing support tickets, and addressing compatibility problems.
- Customer Portal and Monitoring Tools: Leveraging centralized management dashboards and monitoring tools provided by HCI vendors or third-party solutions to track system health, monitor performance, receive alerts, and manage support cases effectively.
- Continuous Improvement and Training: Staying updated with the latest HCI technologies, best practices, and security measures through continuous learning and training programs, enabling them to effectively manage and support Bank's HCI environment.

7. Asset and Volumetric Baseline

Below are the asset details considered for DC & DR Monitoring, Administration & Management support:

Category		DC Site (Instances)	DR Site
Server	Physical	**245**	**170**
	Virtual	**710**	**475**
	Exa-Data / Exa-CC box	**4**	**4**
Database	MS SQL	**60**	**45**
	MySQL	**25**	**20**
	Mongo DB	**5**	**5**
	Postgresql	**5**	**5**
	IBM DB2	**5**	**5**
	Exa-Data / Exa-CC	**5**	**5**
	ORACLE	**125**	**90**
	Total	**230**	**175**
Operating System	AIX	**45**	**45**
	CentOS	**10**	**10**
	ESXI	**30**	**20**
	Linux	**180**	**100**
	Solaris	**120**	**80**
	Oracle Enterprise Linux	**5**	**5**
	Customized OS	**25**	**20**
	RHEL Containerized Instances	**40**	**40**
	Windows	**500**	**325**
	Total	**955**	**645**
Storage	Hitachi- Enterprise Storage Box	**1**	**1**
	Hitachi- Mid Range Storage Box	**1**	**1**
	Hitachi- Enterprise Storage Box at NLS	**1**	**1**
	Total	**2**	**2**
Backup	CommVault Servers/Media Agents & Commcell Servers with Windows 2022	**6**	**6**
	Primary Storage box (with capacity in PB at DC & DR)	**1**	**1**
	HCP Storage Box (with capacity in PB at DC & DR)	**1**	**1**
HSM	Thales/Luna	**7**	**7**
Load Balancers	Radware/A10/F5/Citrix	**4**	**4**

Table 3: Asset Volumetrics

8. Service Delivery Milestones

Milestone	Description	Target Timeline from issuance of PO	Target milestones
1. Project Kick-off	Formal kick-off meeting with Bank's DC & PM team; review of SOW, SLAs, escalation matrix, and project governance plan including but not limited to formal initiation procedure, including resource onboarding plan, finalization of transition plans, and confirmation of deliverables.	Within 10 calendar days.	Kick-off minutes.
2. Deployment of Project Team	Deployment of all required qualified personnel at DC, NLS and DR sites as per resource qualification criteria and post interview by Bank Team (wherever required)	Within 10 calendar days after Project Kickoff.	100% resource deployment with Bank's approval
3. Knowledge Acquisition and Assessment	Review of existing infrastructure, understanding of documentation, backup & restoration processes and operational processes to ensure seamless service transition. This shall also include physical visit to all sites of the bank under scope.	Within 1-month after Deployment of Project Team	Vendor to submit the transition report to bank for sign-off
4. Shadow Activities & Checklist and other Requirements	Service Provider to observe incumbent team/vendors carrying out BAU operations and highlight pendency (if any) during KT in the form of checklist. This will also include preparing a list of gaps, access requirements, and dependencies identified for transition.	Within 15 calendar days after Assessment	Vendor to submit the transition report to bank for sign-off
5. Reverse Shadow Activities	Service Provider team to perform BAU operations under close observation of incumbent Bank team/vendors to demonstrate readiness, accuracy, and process adherence. All deviations and clarifications to be documented and signed off.	Within 15 calendar days after Shadow Activities	Vendor to submit the transition report to bank for sign-off
6. Transition & Handover from Existing Bank Team/ Vendors	Knowledge transfer from incumbent Bank team/vendors; documentation collection (Architecture diagrams, configurations, asset inventory, SOPs etc as per requirement). This shall also include understanding of tools like ITSM, APM, OEM Tool, Workflow Automation, Flexnet etc.	Within 45 calendar days after deployment of Project Team & Resources.	Sign-off by Bank on KT completion checklist. & transition reports
7. DC Operations Takeover & Go-Live at all 3 sites (DC, NLS, DR)	Service Provider assumes complete responsibility for DC operations under SLA framework at all 3 Datacenters of the Bank.	Within 30 calendar days after handover.	Smooth transition without unplanned downtime in line with SLA and service level management. Transition to steady-state operations, including ongoing service management, performance monitoring, and continuous optimization.
8. Documentation & SOP Finalization	Submission of updated SOPs, escalation matrices, DC, NLS, DR run books, Backup and Restoration activity along with its cross checking and asset registers.	Within 15 calendar days after Operations Takeover	All documents to be approved by Bank; version-controlled repository to be maintained.
9. Security & Compliance Audit (Baseline)	Bank shall conduct baseline security posture assessment, asset vulnerability scan, and compliance review.	Within 45 calendar days post previous step or as per Bank's Schedule	Audit report to be submitted; remediation plan to be approved by Bank.
10. Performance Validation & Compliance Testing	Execution of system benchmarking, SLA compliance checks, and disaster recovery drills, Backup restorations at DC & DR.	Within 30 calendar days post previous step or as per Bank's Schedule	All documents to be submitted and Sign-Off to be taken from Bank.
11. Monthly SLA Review	Monthly review meetings with Bank on SLA adherence, incidents, patching, VAPT Closures, Upgrades, Migrations and improvements etc.	Every month	Signed SLA review minutes and action items.

12. BCP testing, & DC-DR Drill	Conduct full-scale DR drill in coordination with Bank. Including Backup shipping/restoration at DR.	Twice a year separately carried for Critical and Non-Critical Setups or as per Regulator Compliance / Bank's Requirement.	RTO & RPO targets to be achieved as per SLA.
14. Annual Security Audit	Conduct comprehensive security audit and submit compliance status.	Annually	Audit passed with remediation actions tracked.
15. Exit Management & Final KT	Smooth handover of operations, documentation, credentials, source codes, and assets to Bank or new vendor at contract end.	Within 90 days before the contract closure date	Exit checklist signed by Bank.

Table 4: Service Delivery Milestones

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 /PBG

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.

9. Location of Work

The successful bidder shall be required to work in close co-ordination with Banks teams during entire life cycle of the project. The successful bidder shall be required to work majorly from the Data Center located in Noida, NCR, along with support across all locations prescribed by Bank. All expenses (travelling/lodging, etc.) shall be borne by the successful bidder.

1. **Data Center Noida**
   Jammu & Kashmir Bank Ltd.
   Green Fort Data Center,
   Plot B7, Sector 132,
   Noida U.P.-201301

2. **Near Line Site**
   Jammu & Kashmir Bank Ltd.
   Nxtra Data Limited,
   B-192, Noida Phase II,
   Near NFEZ Noida, (UP)-201304

3. **DR Mumbai**
   CtrlS Data Center,
   Mahape, Navi Mumbai,
   Maharashtra, 400701

10. 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" 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 RFP Application Fees of **₹5,000** by way of NEFT, details of which are mentioned at clause of Earnest Money Deposit.

Bidders are required to submit Earnest Money Deposit (EMD) for **₹1,25,,00,000/-** (Rupees One Crore Twenty Five Lacs Only). The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 180 days 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.

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

SECTION B - EVALUATION PROCESS

The endeavor of the evaluation process is to find the best fit Solutions as per the Bank's requirement at the best possible price. The evaluation shall be done by the Bank's internal committees formed for this purpose. Through this RFP, Bank aims to select bidder(s) /Service provider(s) who would undertake **DC-DR Monitoring & Management Services**. 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.

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

Stage A. Evaluation of Eligibility
Stage B: Technical Evaluation
Stage C. Combined Quality cum Cost Based System (CQCCBS)
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 qualifying Stage B will 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.

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.

Stage A-Evaluation of Eligibility Criteria

All bids submitted by the participating bidders in this tender shall have to qualify the Eligibility Criteria as detailed in Annexure D of this RFP. Criteria mentioned in Annexure D is the baseline criteria for participation and bidders who do not qualify the criteria will not be considered for Technical Evaluation & Scoring. All the bidders shall be intimated of their qualification status by the Bank once the evaluation of their bids is completed. 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 B-Evaluation of Technical Bid

All technical bids of bidders who have Qualified Stage A shall be evaluated in this stage and a technical score would be arrived at basis of the below table.

Parameters	Marks Allocation	Max Marks
Bidder's Average Turnover (last 3 Financial years)	Annual Turnover: ≥ ₹801 Cr: 10 points Annual Turnover: ₹501–800 Cr: 8 points Annual Turnover: ₹200–500 Cr: 5 points Vendor to submit a Copy of the audited financial statement for required financial years. (Certificate from statutory auditor for preceding/current year may be submitted.)	10

Years of operations in IT/Managed Data Centre Services or similar projects as on the date of RFP (Relevant banking Experience on DC Infrastructure Managed Services and Minimum Head Count: 10) *(Networking experience like NOC/SOC shall not be counted)*	≥ 10 years: 10 points >5–10 years: 8 points 3–5 years: 6 points	10
Project Experience in relevant engagement / Client References in the last 5 years (Relevant Experience on DC Infrastructure Managed Services and Minimum Head Count: 10) *(Networking experience like NOC/SOC shall not be counted)*	≥ 5 Scheduled Commercial Banks: 25 points 4 Scheduled Commercial Banks: 20 points 3 Scheduled Commercial Banks: 15 points Vendor to submit a copy of Purchase Order along with Completion Certificate/ satisfactory Performance Certificate to be submitted as documentary evidence from the relevant Banking clients in India.	25
Email/Virtual/In-Person meeting with minimum **two** client references (for the above provided credentials) to access the level of satisfaction against delivery of services	Bidder's Clients to submit their feedback over official email id provided by the bank within 7 working days. Each client will be asked to rate the vendor's performance on a scale of 0–15 based on the requested criteria. Scores from all available client references will be averaged to arrive at the final score for this criterion. Average Score ≥12/15: 15 points Average Score ≥ 8/15: 10 points Average Score ≥ 5/15: 8 points If fewer than 2 responses are received within 7 days, the bidder will be given 0 points for this criterion.	15
Technical Proposal & Presentation Evaluation (Proposed Service Delivery, Governance Model)	Evaluation will be based on: 1. Understanding of bank's requirements 2. Approach & Methodology, including proposed SLA adherence, monitoring tools, governance process, escalation matrix, and reporting mechanism. 3. Transition plan 4. SLA based Target Operating Model 5. Proposed Team in alignment with the Scope of Work (Section 4 & 5) and Inventory (Section 8). Additionally, specify the proportion of L1, L2, and L3 resources for: • Servers /VMs /OCP Management • OS Management • DB Management • Middleware Management • Load Balancer & HSM Management • AD/DNS Management • Exchange Mail Messaging (Hybrid Model) Management • DR Management Also, pls note, Bidder's proposed team 100% of L1 on bidder's own payroll will get a higher weightage as compared to 80% of L1 on bidder's own payroll.	40

	6. Project Governance 7. Risks & Assumptions 8. Additional Value proposition 9. OEM partnerships 10. Exit Management	

Table 5: Technical Evaluation

Minimum Technical Qualification:
Bidders scoring at-least overall score of 70% score or more will be declared technically qualified.

- The bidder must score ≥ **70% marks** in overall technical evaluation to be considered for commercial bid opening.

Notes:

- All experience and certifications must be supported by documentary evidence.
- Marks under each parameter will be awarded based on submitted proofs, Onsite/Offsite Deliberations with clients and evaluation committee's assessment. Bank's decision in this regard will be final and non-challengeable.

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.

Note: Bank may seek clarifications from 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. The bidders will submit the Technical Bid in the format as per Annexure E. Those Bidders who meet the threshold score of 70 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 will be returned.

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

Stage C- Combined Quality cum Cost Based System (CQCCBS)

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

i. Commercial Bid of only those bidders will be opened who comply with all the eligibility criteria, qualify the Technical Evaluation Stage and confirm compliance to all the terms & conditions and requirements of the RFP document.
ii. The Bank's evaluation of the indicative commercial bids will consider the bidder's compliance with the terms and conditions.
iii. The offer must remain valid for a period of at least 180 days from the date of the tender opening.
iv. Bidders are responsible for the accuracy of all cost computations in their commercial bids. The Bank will review these computations and correct any arithmetic errors identified. While the Bank will make reasonable efforts to identify errors, the ultimate responsibility for accuracy lies with the bidder.

Combined Quality cum Cost Based System (CQCCBS)

i. Under the CQCCBS, technical proposals will be allotted a weightage of **70%,** while financial bids, will be allotted a weightage of **30%.**

ii. The proposal with the lowest cost will be given a financial score of 100, and other proposals will be given financial scores inversely proportional to their prices.

iii. The total score, encompassing both technical and financial aspects, shall be obtained by weighing the quality and cost scores and summing them up. The proposed weightages for quality and cost shall be specified in the RFP.

Highest Point's Basis:

Based on the combined weighted score for quality and cost, bidders shall be ranked in terms of the total score obtained. The proposal achieving the highest total combined score in the evaluation of quality and cost will be ranked as L-1, followed by proposals securing lesser marks as L-2, L-3, and so on. The proposal securing the highest combined marks and ranked L-1 will be invited for negotiations, if required, and shall be recommended for the award of the contract.

Example Procedure:

As an example, the following procedure shall be followed:

While it was decided to have minimum qualifying marks for technical qualifications as 70, and the weightage of the technical bids and financial bids was kept as 70:30. Suppose in response to the RFP, three proposals (A, B, & C) were received and the technical evaluation awarded to them was 75, 80, and 90 marks, respectively. Since the minimum qualifying marks were 75, all three proposals were, therefore, found technically suitable, and their financial proposals shall be opened. For understanding let the financial proposals to be evaluated by the Committee are as under:

Proposal	Technical score	Commercial Bid
A	75	Rs.120
B	80	Rs.100
C	90	Rs.110

Table 6: CQCCBS Example

Using the formula **LEC / EC** (where LEC stands for lowest evaluated cost and EC stands for evaluated cost), the committee shall assign the following points for the financial proposals:

- Proposal A: 100 / 120 = 83 points
- Proposal B: 100 / 100 = 100 points
- Proposal C: 100 / 110 = 91 points

  (Rounded to nearest digit)

Following this, the evaluation committee shall calculate the combined technical and financial scores as follows:

- Proposal A: 75 x 0.70 + 83 x 0.30 = 77.4 points
- Proposal B: 80 x 0.70 + 100 x 0.30 = 86.0 points
- Proposal C: 90 x 0.70 + 91 x 0.30 = 90.3 points

Based on the combined technical and financial evaluation, the three proposals were ranked as follows:

- Proposal A: 77.4 points - L3
- Proposal B: 86.0 points - L2
- Proposal C: 90.3 points - L1

Proposal C, with an evaluated cost of Rs. 110, will therefore be declared the winner and recommended for negotiations/approval to the competent authority.

SECTION C - RFP SUBMISSION

1. 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) Publishing of RFP
b) Vendor Registration
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) Commercial Evaluation
k) Contract Award

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

2. 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:

Contact Persons: Nandan Velara
Mobile No.: 9081000427 / 9904407997
Landline: 079-68136831/ 6857 / 6820 / 6843 / 6853 / 6829 / 6835 / 6863 / 6852 / 6840

No consideration will be given to e-Bids received after the date and time stipulated in this RFP and no extension of time will normally be permitted for submission of e-Bids.
Bank reserves the right to accept in part or in full or extend or reject the bids received from the bidders participating in the RFP.
Bidders will have to abide by e-Business Rules framed by the Bank in consultation with M/s. e-Procurement Technologies Ltd.

3. RFP Fees

The non- refundable RFP application fee of Rs. 5,000/- is required to be paid by the prospective 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 5,000/=

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.

4. Earnest Money Deposit

Prospective bidders are required to submit Earnest Money Deposit (EMD) of ₹ 1,25,00,000 (Rupees One Crore Twenty Five lacs Only).The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 180 days 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 1,25,00,000/-

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 H.
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:	Technology & Development Department, J&K Bank Ltd. 5th Floor Corporate Headquarters M.A Road Srinagar J&K Pin- 190001

The EMD submitted 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 contract value for 5 years and valid for 5 year+6 months including claim period of 6 months, validity starting from its date of issuance. The PBG shall be submitted within 30 days of the PO issued from the Bank.
b. The Unsuccessful Bidder, only after acceptance of the PO by the selected L1 bidder.

5. Performance Bank Guarantee (PBG)

The successful bidder will furnish unconditional performance bank guarantees (other than Jammu & Kashmir Bank) from any scheduled commercial bank in India, for 5% of the total contract value for a period 5 years + 6 months. The format of the PBG is given as per Annexure I. The PBG shall be submitted within 30 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 favour 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.

6. 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 and EMD details mentioned above.

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 under each Scope /Section will be arrived post technical evaluation followed by CQCCBS among the technically qualified bidders. After CQCCBS, 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, the Successful Bidder (L1) shall submit to the Bank the price breakup for the bid amount in the format as provided by the Bank. If the price breakup is not submitted to the Bank within 7 days from the date of the declaration, the Bank reserves the right to reject 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. This contract will be awarded initially for a period of five (5) years from date of signing the contract & shall be further extended if both parties wish to continue on the same terms of service.

vii. 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 along with invoking the submitted PBG/EMD. Bank's decision in this regard will be final.

viii. 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 shortlisted vendors after giving 15-days‟ notice to the defaulting Vendor. Also during the period of the contract due to unsatisfactory service, Bank will have the right to cancel the contract and award the contract to other participating vendors.

7. Bidding Process

i. The bids in response to this RFP must be submitted in two parts:
   a. Confirmation of Eligibility Criteria
   b. Technical Bid‟ (TB) and 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 & suffice the minimum Technical Evaluation criteria will be qualified for techno-commercial bid evaluation. The successful Bidder will be determined based on the CQCCBS calculation as described in the relevant section of the RFP.

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.

8. 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.

9. 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 the commercial bid shall remain valid for duration of 06 calendar months from the date of declaration of L1 Bidder.
iii. Once Purchase Order or Letter of Intent is issued by the Bank to L1 Bidder, 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.

10. Bid Integrity

Wilful 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.

11. 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.

12. 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 of Bidders and shall be summarily rejected.

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**.

13. 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.

14. Payment Terms

The Bidder must accept the payment terms proposed by the Bank as proposed in this section. The indicative commercial bid submitted by the bidders must be in conformity with the payment terms proposed by the Bank.

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

Category	Description	Payment Payout w.r.t Total TCV Amount	Billing Frequency	Penalty Applicability
Contract Signing & Project Kick-off	Payment post Signing the contract, Initial planning and assessment along with mobilization/ deployment of resources	**5%**	One Time	Not Applicable
Mobilization of Resources	Deployment of all required qualified personnel at DC, NLS, DR, as per resource qualification & experience years criteria shown in the RFP (Post interview by Bank Team wherever required)	**5%**	One Time	SLA-linked penalty on domain fee
Service Commencement / Go-Live at all 3 sites (DC, NLS, DR) along with base Audit Completion and Starting of all BAU Activities (as defined in the RFP) with Monthly SLA Compliance	Upon Successful start of SLA-Based BAU operations including servers, storages, databases, application administration, BCP Activities, Backup shipping /restoration etc. Linked to SLA Performance: Uptime, incident response, change management, patching, backup success, storage performance, monitoring and reporting.	**90%**	**Quarterly in Arrears** post Governance & review meetings with Bank on SLA adherence, incidents, RACs, Upgrades, hardening, Patching, VAPT Closures etc. Detailed Reports to be submitted to the Bank in support of Uptime commitments against each BAU Activity separately.	SLA-linked penalty on domain fee
Rate Card for Ad-Hoc Projects	Cloud to On-Prem - Major migration projects Hyperconverged Infrastructure deployment and configuration	Per Project Mutually agreed between bank and MSP with Indicative Prices as given by the MSP taken as reference.	Based on Mutual Agreement	NA

Table 7: Payment Schedule

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

- No advance payment will be made on award of the contract.
- One -Time or Quarterly in arrears on submission of invoices and Uptime Reports duly signed by the Bank's Governance team/Or Official Concerned, after deduction of penalties/charges / Liquidated damages (if any) mentioned in the agreement.
- All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.

- Payments will be withheld in case of Non-compliance of the terms and condition of this RFP.

Payments shall be released on acceptance of the purchase order and:

a. Post Signing of Service Level Agreement (SLA) between Bank and Successful bidder.
b. Post Signing of Non-Disclosure Agreement (NDA) between Bank and Successful bidder.
c. All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.
d. No Payment shall be made for the transaction processed beyond the timelines.

General Principles

1. Payments against all BAU Activities shall be made on a **quarterly in arrears** basis, subject to:
    - Verification of service delivery against agreed SLA parameters.
    - Submission of all required reports, invoices, and supporting documents.
2. All payments will be linked to **SLA compliance**. Any penalty due to SLA shortfall will be deducted from the corresponding quarter's payment. (Please refer to Annexure J for SLAs & Penalties)

Invoice & Documentation

- Invoices must be submitted within **15 days** after the quarter end.
- Invoices must be accompanied by:
    - Monthly SLA compliance reports (signed by Bank's authorized official).
    - Incident & RCA reports for Severity 1/2 issues.
    - Preventive maintenance and patching, Vulnerability Closure reports.
    - Backup/DR drill completion reports.

Bank's Rights

- The Bank reserves the right to withhold part or full payment in case of:
    - Disputed SLA compliance metrics.
    - Pending RCAs for critical incidents.
    - Non-completion of agreed preventive maintenance, Vulnerability Closure activities.
- Any withheld payment will be released after the Service Provider rectifies the breach and provides evidence of compliance.

D - GENERAL TERMS & CONDITIONS

1. 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.

2. 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.

3. 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.

4. Liquidated Damages

If successful bidder fails to make delivery or 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 every 1 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.

5. Fixed Price

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

6. Right to Audit

Bank reserves the right to conduct an audit/ ongoing audit of the services provided by Bidder (including its sub-contractors). The Selected Bidder shall be subject to annual audit by internal/ external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India 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 Bidder is required to submit such certification by such Auditors to the Bank.

Bidder should allow the J&K Bank or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Bidder and business premises relevant to the outsourced activity 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. Bidder should allow the J&K 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.

7. 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, 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.

8. 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.

9. Amendments

Any provision 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.

10. Assignment

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

11. 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.

12. 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 and designated representative of the Bidder. If designated Officer of the Bank and representative of Bidder, for the selection of DC-DR Monitoring & Management Services, 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.

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

The Successful Bidder shall have to execute service level agreement capturing details of the activity being outsourced, including appropriate service and performance standards including for the sub-contractors, if any for deliverables including Service-Level Agreements (SLAs) formalizing performance criteria to measure the quality and quantity of service levels 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 30 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.

14. '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.

15. 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.

16. 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.

17. 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.

18. 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 including sub-contractors shall follow J&K Bank's information security policy , Supplier 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 and storage of data (as applicable to the concerned REs) only in India as per extant regulatory requirements.

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. Successful Bidder shall comply with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data

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.

19. 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 payments receivable under and in accordance with that business.

20. 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.

21. 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.

22. Corrupt and Fraudulent practice:

i. It is required that Successful Bidder 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 Successful Bidder 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.

23. Solicitation of Employees

Neither Bidder nor J&K Bank shall hire employees of J&K Bank/Bidder or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of each other directly involved in this contract during the period of the contract and one year thereafter.

24. 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.

25. Confidentiality Provision

a) 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.

b) 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.

26. 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 without prior written consent from the Bank. All the resources deployed by the bidder should be on the bidder's payroll.

27. 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.

28. 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.

29. Taxes and Duties:

i. 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.
ii. 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.
iii. Tax Deduction at Source: Wherever the laws and regulations require deduction of such taxes at source of payment, Bank shall effect 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 Bidder in respect of this contract.

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.

SECTION E - ANNEXURES

Annexure A: Confirmation of Terms and Conditions

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank MA Road, Srinagar

Dear Sir,

Sub: RFP No …… **Selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR).**

Dated ……

Further to our proposal dated ....., in response to the Request for Proposal **for Selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)** hereinafter referred to as "RFP") issued by 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 be submitted under the letter head of the bidder company and signed by Authorized Signatory)

The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank M.A Road, Srinagar

Dear Sir,

Sub: RFP no: _____ **Selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR),** dated _____

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer **Selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)** 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, 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 Service Provider

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

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	Name & Address of System Integrator	
12	Brief Description of after sales services facilities available with the SI/OEM	
13	Web Site address of the Company	

Date:

Seal and signature of the bidder

Annexure D: Compliance to Eligibility Criteria

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

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:

1. Legal & Regulatory

Criteria	Requirement	Documents to be Submitted	Compliance (YES/NO)
Legal Entity	The bidder must be a registered company in India under the Companies Act, 1956/2013 or a registered Govt Organization/ PSU / PSE/ LLP or Private/ Public Limited Company in India. The Company should have been in existence in India for a minimum period of 4 years.	Certificate of Incorporation / Registration	
Years in Operation	Minimum 3 years of operations in IT/Managed Data Centre Services as on the date of RFP publication. Bids under consortium arrangement are not allowed.	Incorporation certificate + Relevant POs/Work orders	
Compliance	Must not be blacklisted, debarred, under investigation by any Government/Central/State Govt./PSU/BFSI institution in India.	Self-declaration on company letterhead against each signed by authorized signatory	
	The Service Provider should not be part of any sanctions or negative list.		
	Service provider should not have been flagged / fined for non-compliance with rules.		
Statutory Registrations	Must have valid PAN, GST Registration, and comply with all applicable labour laws.	Copies of PAN, GSTIN, PF, ESIC certificates	

2. Financial Strength

Criteria	Requirement	Documents to be Submitted	Compliance (YES/NO)
Annual Turnover	The Bidder must have registered an average annual turnover of ₹200 crore or more during the last 3 financial years as on date of RFP (Not inclusive of the turnover of associate companies).	Audited financial statements & CA certificate	
Profitability	The bidder must have a Positive Net Worth in last 3 financial years as on date of RFP.	Audited financial statements & CA certificate against all FYs.	
Solvency & Bankruptcy	The Bidder should not be involved in any legal case that may affect the solvency / existence of firm or in any other way affect the bidder's capability to provide / continue the services to Bank. NOR The Bidder should not have filed for Bankruptcy in any country.	Self-declaration Confirming the criteria.	

3. Technical Capability

Criteria	Requirement	Documents to be Submitted	Compliance (YES/NO)
Experience	The bidder should have executed/ongoing minimum of three (3) projects of DC Management in Scheduled Commercial Banks in the last five years with each project value ≥ ₹5 Crores.	Bidder must submit the detailed client references at the time of bid submission. Bidder must also submit relevant Purchase Orders (POs)/ Contracts/ letter of award and letter of providing satisfactory performance/ completion certificates from clients, confirming the bidder's experience along with contact details of the firm for verification.	
Technical Criteria	The bidder should comply to the defined technical criteria (as per annexure E)	Submission of Annexure E	
Data Centre Expertise	Experience in managing Tier-III or higher-rated Data Centres involving the compute infrastructure and allied services hosted at the premise in India.	Client references	
Manpower Strength	Minimum 100+ technical resources on its payroll, with at least 30+ resources certified in relevant technologies to manage this SLA based data center management project with all compliances.	Self-declaration on letterhead along with payroll records or HR certificate specifying the number of certified DC engineers with qualifications.	

4. Certifications & Compliance: Bidder should mandatorily have below certifications and must show compliance to below Laws & Statutes.

Criteria	Requirement	Documents to be Submitted	Compliance (YES/NO)
ISO:27000 or ISO/IEC 27001 Series	Information Security Management certification (Certification must be valid for the entire contract period)	Copy of certificate	
ISO 20000	IT Service Management certification (valid).	Copy of certificate	
Compliance to Laws & Statutes	The Bidder shall ensure full and strict compliance with all applicable laws, statutes, rules, regulations, directions, guidelines, and notifications issued by any statutory, regulatory, or governmental authority having jurisdiction in India, including but not limited to those promulgated by the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI), Ministry of Electronics and Information Technology (MeitY), and any other sectoral regulator, as may be applicable to the scope of services under this RFP. The Bidder shall also be responsible for complying with all relevant provisions of the Information Technology Act, 2000 (as amended), Data Protection and Privacy Laws including the Digital Personal Data Protection Act, 2023, labour laws, taxation laws, contractual laws, and any other legislation that may be applicable from time to time. The Bidder must ensure adherence to globally recognized standards and frameworks governing technology services, information security, and service	Self-declaration + process documents	

	management, including but not limited to ISO/IEC 27001 (Information Security Management System), ISO/IEC 20000 (IT Service Management), ISO/IEC 22301 (Business Continuity Management), ISO/IEC 27701 (Privacy Information Management), and any other standard or best practice as may be deemed relevant and applicable to the nature and scope of the engagement. It shall be the sole responsibility of the Bidder to monitor, interpret, and ensure compliance with all such statutory, regulatory, and standardization requirements throughout the term of the contract. Any non-compliance, whether wilful or inadvertent, shall be construed as a material breach of the contractual obligations and shall render the Bidder liable to penalties, corrective action, or termination as per the terms of the RFP and subsequent agreement.		

5. Local Presence & Support

Criteria	Requirement	Documents to be Submitted	Compliance (YES/NO)
Resource Expertise	The bidder must ensure that at all proposed resources/ team members meet the following minimum experience requirements in Data Center management: • L1 Support: Minimum 2 years of relevant experience with minimum Foundation and or Intermediate level OEM Certification in particular Domain • L2 Support: Minimum 4 years of relevant experience with minimum Intermediate level OEM Certification in particular Domain. • L3 Support: Minimum 6 years of relevant experience with Advanced/Expert Level OEM Certification in particular Domain.	Self-Signed Certificate	
Local Office	Fully functional office in India, with full-fledged operational offices in Delhi & Mumbai.	Address proof + GST registration	
24×7 Support	Capability to provide 24×7 on-site & remote support with escalation matrix.	Self-declaration + resource plan+ Escalation matrix separately for DC, NLS & DR	

6. Additional Requirements

Requirement	Compliance (Yes/No)
The MSP should be willing to sign SLA, NDA with the bank & submit the required PBG with the Bank.	
Should be ready to transition existing DC operations with zero downtime.	
Must agree to SLA-bound penalties as defined in the RFP.	

Pls Note: All documentary evidence/certificates confirming compliance criteria should be part of eligibility criteria and must be signed by the authorized signatory of the Bidder. 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.

1. Bidders need to ensure compliance to all the eligibility criteria points.
2. Scheduled commercial Banks / PSU Banks do not include Regional Rural Banks and Cooperative Banks.

Annexure-E: Compliance to Technical Criteria

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

Please mention 'Y/N' in the last column as per the availability of the parameters.

Indicator	Description	Marks
Yes	Supporting documents are to be submitted and/or points will be verified during presentation or onsite visit. If found not complied marks will be reduced accordingly or as per discretion of the Bank.	1
No		**0**

Technical Criteria	Max Score	Compliance (Yes/No)
5.1. Server Management (OS Management & Virtualization Management)		
5.1.1. Monitoring		
Perform monitoring of all the servers in the Customer's data centres and Near Line Site, for the following parameters by polling the servers at pre-defined intervals:		
- Availability of the server	1	
- File System / Partition Utilization as applicable	1	
- Virtualization	1	
- Memory utilization	1	
- Processor utilization	1	
· Managing Disk space network Utilization related to server		
- Monitor CPU, Kernel, Disk, Memory, I/O and all other important System parameters	1	
Monitor critical services related to operating systems and performance tuning.	1	
Configuring monitoring and alerting systems, including periodic event log analysis and investigation of recurring incidents to maintain server integrity	1	
Verify system/storage logs and periodically clean up log files/mount points	1	
Inform bank of any impending problems which can potentially lead to system crash or performance degradation and preparing Major Incident Reports (MIR) along with RCA for significant incidents.	1	
Log tickets in the helpdesk tool for valid alerts	1	
Incident / Request Fulfilment / Change management	1	
Conducting periodic audits in cages for the servers & assets for proactive maintenance and extending hardware lifespan.		
i. Monitor Physical Hardware in the cage area for any anomaly, malfunctioning and amber. Intimate Bank Team for logging case with the respective Vendors/OEMs for replacement of failed drives and parts.	1	
ii. Capturing logs as per OEM requirement and raising the SRs or Calls along with requisite logs on OEM portal. Coordinate with the OEM resource till RMA call is resolved.	1	
5.1.2. Server Administration		
Create, modify and delete user groups, users and user properties	1	
Managing network shares, terminal services, cluster services, and file servers, including creation, modification, deletion, and reconfiguration as needed.	1	
Assign user access rights as per policies defined and agreed upon with the Customer, including account policies like password length, age, and administrator/supervisor password restriction	1	
Assign space usage restrictions and manage disk space, volume groups, and server resource utilization (disk, processor and network etc).	1	
Configure and maintain print servers, print queues, terminal services, cluster services, and file servers.	1	
Maintain and administer DNS, DHCP (including scopes and reservations), NFS, NIS, DFS roots, group policy, and file system mounts.	1	
Restore server operating system in the event of a crash using backup tools as provided by customer or proposed as part of solution	1	

Resolve server problems like system hang, hard disk crash, with OEM support wherever required	1	
Create new file systems and correct file system inconsistencies as and when required	1	
Installation, configuration, and administration of file systems, volume managers, including LVM administration.	1	
Configure the print servers, terminal services, cluster services, and file servers.	1	
Perform periodic system performance tuning as per Customer's policy	1	
Perform periodic schedule maintenance activity	1	
OS & Server Hardening and Patching as and when released by OEM or as per patching cycle. Firmware upgrades for hardware as and when released by OEM.	1	
Implementation of Audit/VAPT recommendations	1	
Installation, reinstallation, upgrade, and migration of the operating system as required or due to incidents	1	
Configuration and administration of OS, Logical partitioning of LVM, and HA configuration. Cluster Administration(HACMP) /Installation/Re-installation	1	
Backup of Operating System, Vhdx, root backups, BMRs etc.	1	
Commissioning and de-commissioning of servers	1	
Server Reinstallation and configuration due to Incident	1	
Managing server build and provisioning with or without automation tools	1	
Creation of shell scripts or batch programs to automate certain procedures	1	
Capacity Management & augmentation with respect to CPU and RAM along with intimation to Bank for any best practices and recommendations.	1	
Adding servers to the clusters (Active-Active & Active-Passive Clusters) and configure, monitor and maintain the cluster functioning as per requirement.	1	
Migration of server VMs or application Servers/VMs hosted on EOSL hardware to new Hardware with same or upgraded compute configuration and with or without OS, DB and Middleware Upgrade.	1	
Co-ordinate with SSL Certificate vendor/Bank for issuing and deployment of SSL certificates and further timely deployment of the same	1	
Carry out DC-DR Drills to meet Regulatory Compliances within defined RTO and RPO times including Server pre-checks and monitoring for smooth switchover & switchback.	1	
Timely closure of the identified OS/ database/middleware vulnerabilities.	1	
Implements and enforces security/baseline for all OS as per the hardening document of the Bank	1	
Password management of super users (e.g., root/support) and defining account policies, including password length, age, and administrator/supervisor password restrictions	1	
Schedule and execute cron jobs and fine tune same under Bank's intimation and approval.	1	
Creation of shell scripts or batch programs to automate certain procedures	1	
Patch Management (Update / Preview / Rollback)	1	
Firmware Management [Upgrade/Downgrade] of HCI/servers/appliances/storages /switches.	1	
Perform periodic schedule maintenance activity	1	
Server Snapshot management	1	
Implement and manage Linux messaging and security solutions to ensure secure communication and compliance.	1	
Monitor and manage console access to servers, ensuring secure and controlled access.	1	
Configure and manage Logical Partitioning (LPAR) and Hard Partitioning (HPAR) for optimal server performance.	1	
Maintain trusted execution environments for file integrity checks and malware protection.	1	
Configure encrypted file systems to protect sensitive data as per security standards.	1	
Administer IBM Hardware Management Console (HMC) for efficient server hardware management.	1	
Perform trend analysis on historical performance data for capacity planning and forecasting.	1	
Conduct regular vulnerability scanning of all servers and VMs in addition to patching.	1	
Monitor and alert on the health of hardware components on physical servers and virtualization hosts (e.g., fans, power supplies, temperature, disks).	1	
Antivirus/antimalware updates and endpoint protection management.	1	

Antivirus/antimalware installation, updates, and monitoring.	1	
Recommendations for hardware upgrades, consolidation, or virtualization.	1	
Customization of OS builds for specific workloads.	1	
5.1.3. VM Monitoring		
Monitoring Virtualization Host servers for availability	1	
Monitoring Virtual Machines hosted on the Virtualization host for availability	1	
Basic VM provisioning and de-provisioning tasks	1	
Managing hypervisor configurations (VMware, Hyper-V, KVM etc.)	1	
VM Cluster Functioning, Monitoring and Management egs: HACMP	1	
Optimizing resource allocation (CPU, RAM, storage)	1	
Monitoring of performance metrics like CPU, Memory of Virtualization host server	1	
5.1.4. VM Management		
Creating, modifying, deleting Virtual Machines (VMs)	1	
CPU & Memory resource allocation to VM	1	
Troubleshooting issues with Virtualization Host servers & VM	1	
Migration of VM from one host to another or from One Base machine to another.	1	
Data store migration	1	
Template creation & cloning of VMs along with migration onto other hardware with same or upgraded compute configuration.	1	
Hardware /Virtualization OEM Vendor co-ordination	1	
VM performance tuning	1	
Virtualization Host patch management	1	
P2V , Physical to VM conversion or vice versa	1	
Upgradation of virtualized software	1	
Advanced troubleshooting of hypervisor kernel and networking issues	1	
Integrating cloud-based virtualization (Azure, AWS, GCP)	1	
Environment provisioning and configuration	1	
VM Snapshot management	1	
5.1.5. Open Shift Cluster Containerization Support		
· Resource Allocation: Allocate proper CPU/Memory request C Limits for each POD & also defining the Resource quota at Namespace level. Resolving issues related to insufficient resources, such as CPU, memory, or storage within the OpenShift environment. Configure, modify & set project quotas and limit ranges.	1	
· Cluster Health Monitoring: Check cluster utilization and share reports to Bank when needed. Identifying and resolving performance degradation or resource bottlenecks in OpenShift clusters. Resolve issues with pods like crash loop backoff, image pull back and other errors. Forecast capacity growth requirements and intimate bank for augmentation and handle capacity increase. Perform health checks of the cluster and fix issues based on observations.	1	
· Logs and Metrics Analysis: Collecting and analysing logs from OpenShift and Kubernetes components to diagnose issues or performance problems. Retention of various logs (i.e. App Logs, Audit Logs, Infra Logs).	1	
· Configuration Tuning: Adjusting configuration settings for optimal performance (e.g., tuning resource requests and limits, configuring storage classes). Troubleshooting problems related to pod creation, deployments and scaling.	1	
· Cluster Settings & Troubleshooting: Troubleshoot issues with master/worker/infra/bastion nodes, maintenance and scale-out tasks. Assisting in fine-tuning settings, adjusting pod deployments, storage configurations, and service accounts.	1	
· Issues: Troubleshooting connectivity issues, including problems with ingress controllers, or DNS.	1	

· Handling Patch Updates: Installing minor patches or updates to the OpenShift platform and container runtimes. Deployment of latest OS patches on Bastion, Master, Infra, Worker, and Mirror Registry servers.	1	
· Version Upgrades Assistance: Upgrading to newer OpenShift versions and fixing issues post-upgrade (if any).	1	
· Root Cause Analysis: Analysing complex, intermittent, or critical issues that affect the overall system's availability or performance. Identifying the underlying causes of complex problems, such as persistent failures, systemic issues in application workloads, or systemic network problems in the OpenShift platform.	1	
· Upstream Bug Fixes: Identifying, diagnosing, and working with Red Hat's engineering team or the upstream community to fix critical bugs or vulnerabilities in OpenShift or Kubernetes components.	1	
· Custom Kernel or Software Debugging: Resolving issues that involve debugging, such as kernel panics, performance regressions, or complex multi-node failures that affect the availability of the entire OpenShift cluster.	1	
· Users and User Roles: Create, modify and delete projects/roles. Assign project specific roles to users/groups. Add/remove users and assign roles to group/users. Service account mgmt., role creation and assigning roles.	1	
· Authentication/Authorization Problems: Highlight & Resolve issues related to Role-Based Access Control (RBAC), such as improper permissions or security policies. Troubleshooting user authentication issues and resolving problems with integrated identity providers.	1	
· DR Drills; DC to DR switchover switchback activities with respect to OpenShift cluster. Production cutover and rollout readiness from OCP.	1	
5.1.6. Email Management		
Daily tracker on the Creation / Deletion of the Users	1	
Daily monitoring of MS-Exchange services health alerts and on time reporting to CSB team and to OEM support team for issues	1	
Respond to users' emails in stipulated time for acknowledgement	1	
Management of MS-Exchange Users (Creation/deletion/Unblock/block/Password reset) and Exchange servers (Mailbox Servers, Mail Routing servers etc.)	1	
Daily operations (Content filtering/ attachment restrictions etc.)	1	
End user Outlook profile creation & troubleshooting	1	
Write and maintain documentation for procedures, processes, SOP's, run book, knowledge sharing and configurations	1	
Provide ITSM support by handling all types of tickets, including Incident / Request Fulfillment / Change management	1	
Reports should be submitted as per bank's discretion	1	
· Monthly Mailbox Creation / Deletion	1	
· Health Status report of Exchange Servers	1	
MS-Exchange on premises server administration, monitoring and management	1	
OS patching related required support	1	
Management of End to end, DR drill of MS-Exchange	1	
Set up MS-Exchange standard and best practices in line to the bank requirement	1	
Troubleshooting of daily operational issues on Mailing, connectivity and mobility etc	1	
Closing of compliance and audit points related to email system	1	
Maintain a high level of availability for all MS-Exchange services	1	
Collaborate with other IT teams to troubleshoot and resolve technical issues	1	
Assistance during any production issue related to MS-Exchange and its components	1	
Creation and administration of MS-Exchange rules & policies	1	
Administration of bulk email solution (name of the bulk email platform)	1	
Configure and manage calendar free/busy sharing to facilitate seamless scheduling	1	
Configuration of TLS/SSL encryption for secure mail communication.	1	
Provide advanced troubleshooting for front-end/back-end configurations, including OWA, RPC/HTTP, and ActiveSync	1	
Implement and enforce MS-Exchange standard configurations and best practices in alignment with the bank's security and compliance requirements	1	

Lead the implementation, rollout, and administration of MS-Exchange services, ensuring high availability and security	1	
Manage and optimize hybrid MS-Exchange environments, integrating on-premises and cloud-based identity solutions	1	
Oversee compliance and protection management like retention policies, filters, DLP, quarantine	1	
Fine tuning security parameters of all workloads of MS-Exchange	1	
Implementation and decommissioning of Exchange servers	1	
Suggest new improvements in existing setup	1	
Compliance Management	1	
Journal rules/databases/mail boxes/end user request Management.	1	
Exchange Database / DAG management	1	
User mail box issues.	1	
Public Folders/ users Management.	1	
Managing different rules on Exchange.	1	
Integration with other Devices/ Applications	1	
Distribution Groups creation, member/user and Access Management	1	
5.1.7. Active Directory Management		
Manage pre-created directory structures	1	
Manage domains & domain objects	1	
Monitoring & Management of Active Directory Replication	1	
Monitoring and troubleshooting of network connectivity of all servers	1	
Implement and Manage Enterprise Group Policies	1	
Modification in directory structure if required	1	
Enhancing AD security with conditional access and zero-trust models	1	
Designing AD architecture and domain forest strategies	1	
Implementing identity federation and hybrid AD solutions	1	
Integrating AD with cloud-based identity providers (Azure AD, Okta)	1	
LDAP for centralizing user/group management	1	
Perform backup and recovery of AD servers and AD objects	1	
Perform the addition of servers to the domain as per defined policies and procedures.	1	
Identify and resolve domain-related issues to ensure seamless operation and connectivity.	1	
Update and manage DNS records to maintain accurate and efficient domain name resolution.	1	
Configure and maintain DHCP settings to ensure proper IP address allocation and network functionality.	1	
Administer Active Directory (AD) sites and services to optimize replication and network performance.	1	
Perform monitoring and analysis of server logs to identify and address potential issues proactively.	1	
Under Federation Services Management: ADFS (End –to end maintenance of ADFS servers/users/access management.)	1	
Administration of FSMO roles and AD schema updates.	1	
Enforcement of password policies, account lockout policies, and multi-factor authentication (MFA) integration.	1	
Regular optimization of AD replication and Exchange database performance.	1	
Capacity planning for mailbox storage, AD object growth, and database sizes.	1	
Recommendations for upgrades and performance tuning.	1	
5.2. Database Management		
5.2.1. Database Monitoring		
Perform monitoring of standard critical parameters for the database (monitoring of which is supported as per the deployed DB license) during the service window agreed in this SOW such as:	1	

- Table spaces & database objects and segments.	1	
- Mount points of logs and data files	1	
- Availability of background processes	1	
- Buffer cache utilization	1	
- Highlighting Resource intensive queries through AWR reports along with their impact & RCAs	1	
- Fragmentation of table spaces indexes	1	
- Memory, I/O, CPU utilization for the RDBMSs monitored at OS Level	1	
- Machine Availability	1	
DB-Application Parameters:	1	
JVM Heap utilization	1	
JVM Garbage Collection Time	1	
Sync connection	1	
Total Defunct Processes	1	
Overall Application Average Response Time	1	
DB Server Parameters:	1	
CPU Usage	1	
Disk free space	1	
DiskSpace Utilization	1	
Swap Usage	1	
Uniser Monitoring	1	
Load Average	1	
Analytics agent	1	
CPU Utilization	1	
Average Active Connections	1	
Database Warning	1	
Queues and Waits	1	
IO Requests	1	
Active and Defunct or Lock Sessions	1	
Invalid Object Count	1	
Active & Archive Files Size Check	1	
User Account Lock	1	
Long running query	1	
DB Log Parameters:	1	
Alert logs for errors	1	
Database backup Logs	1	
Transaction Logs	1	
System Errors	1	
Instrumentation Logs & Errors	1	
Monitor system performance and provide performance data to Customer as per requirement	1	
DC and DR sync verification, either manually or through the customer provided tool if sync check is automated.	1	
Monitoring & taking corrective actions (in coordination with Bank Team) for Replication technologies like Oracle Data Guard (ODG), Active Data Guard (ADG), Storage Replication, Synchronous & Asynchronous Replication, SQL Server Replication functioning and related parameters.	1	
5.2.2. Database Administration		
Create, modify and delete database and database objects	1	
Create, modify and delete users and properties	1	

Create, modify and delete maintenance jobs	1	
Perform periodic database performance tuning as per the documented procedures	1	
Perform periodic house-keeping of Database	1	
Perform orderly start-up and shutdown of database services	1	
Add, modify and delete permissions to database objects and troubleshoot user logins	1	
· Cache Optimization	1	
Rectify database configuration problems	1	
Based on Customer's policy provided during transition:	1	
- Perform regular defragmentation, truncation & partitioning activities for better space management and performance tuning.	1	
- Grant and revoke database access to users	1	
- Execution of scheduled database jobs	1	
Database performance tuning and response monitoring	1	
Creation of shell scripts or batch programs to automate certain procedures	1	
Carrying DC- DR drills as per the SOP or through Workflow tools (as per availability).	1	
Upgradation of databases to higher stable versions.	1	
Implementation and configuration of the replication setup for DR and near site, monitor the sync status (Synchronous & Asynchronous), Storage Replication.	1	
Housekeeping on DR server & cleaning up of Archive logs and Alert logs/transaction logs	1	
Assisting in backup and restoration tasks as per Bank's requirement.	1	
Coordination with the OEM Vendors for Product Bugs and Support	1	
Install Database Software along with Database Hardening / Database Patching.	1	
DB Hardening and Patching as and when released by OEM or as per patching cycle.	1	
Microcode upgrades for DB hardware as and when released by OEM.	1	
Troubleshooting deep-level database engine issues	1	
Working with application teams to improve database efficiency	1	
Cluster Management (HACMP)	1	
Architecting high-availability (HA) and disaster recovery solutions	1	
Re-build DC and/or DR instance from available backup in case of crash & Restoring OS from MKSYS backup.	1	
Troubleshoot and resolve RAC (2 node or 3 node) issues and partitioning-related issues to ensure database availability and performance.	1	
Perform import, export, and archival of databases to support data migration and backup processes.	1	
Execute and manage various types of database backups for all applications to ensure data integrity and recovery.	1	
Perform database native backup operations, including RMAN, to maintain data protection and recovery readiness.	1	
Ensure Database and Application backups are in place as per Bank's policy/requirement and resolve database crashes and perform rebuilds as required to restore database functionality.	1	
Resolve database backup issues (if any) and perform rebuilds as required to restore database functionality.	1	
Troubleshoot and resolve unexpected database instance hangs or terminations to ensure continuous operation.	1	
Conduct session-level audits to monitor and ensure compliance with database access and usage policies.	1	
5.3. Middleware		
5.3.1. Proactive Monitoring		
Monitor web server and middleware server availability	1	
Monitor availability of the services deployed in the web server and middleware servers	1	
Monitor alert notifications, check for impending problems, triggering appropriate actions	1	
Monitor client connection status	1	
Monitor threshold values for key parameters such as memory usage, file system usage	1	

Performance tuning and troubleshooting middleware failures	1	
Load/stress testing and tuning of middleware configurations.	1	
Optimize performance for application-middleware-database integration.	1	
Assisting in application deployment following runbook procedures	1	
Managing user access and authentication for middleware services	1	
Managing SSL certificates for middleware components	1	
Implementing advanced security configurations and encryption techniques	1	
Monitor middleware resource use such as connection pooling	1	
Monitor CPU, memory, heap, garbage collection, thread pools, and connection pools.	1	
Audit and monitor middleware logs for suspicious activity.	1	
5.3.2. Administration		
Perform start up and shutdown of web/middleware server instances	1	
Provide support for known errors and problems	1	
Escalate calls as per the escalation matrix	1	
Coordinate with escalation team to close calls	1	
Update knowledge base on closure of a call	1	
Coordinating with application and security teams for compliance adherence	1	
Troubleshooting deep-level middleware performance and integration issues	1	
Log calls based on the monitoring alerts	1	
Raising change requests related to Middleware Services	1	
Manage clustering, load balancing, and failover configurations.	1	
Backup all middleware configurations, security certificates, and related artifacts.	1	
Maintain up-to-date configuration documentation.	1	
5.3.3. Installation and Configuration		
Perform pre-Installation tasks during crash recovery process and for new installations	1	
Perform web server and middleware server configuration (e.g., WebLogic, JBoss, Tomcat, WebSphere) during a crash recovery process and for new installations	1	
Deploying patches and upgrades for middleware applications	1	
Configuring and maintaining middleware services (e.g., WebLogic, Tomcat, JBoss, MQ environment variables, JVM parameters, memory settings.)	1	
Implementing automation for deployments and configurations	1	
Architecting middleware solutions for high availability and scalability	1	
Designing and optimizing enterprise middleware infrastructure	1	
Version and build management for middleware components.	1	
Implement security hardening measures for all middleware platforms.	1	
5.4. HSM & Load Balancer		
5.4.1. HSM & Load Balancer Administration and Management		
Installation-reinstallation, configuration and management of Load balancers.	1	
Troubleshooting the end to end connectivity and flow between the HSM & Load balancer devices and backend servers	1	
Load Balancer Management (creation of Virtual Service, mapping the servers, Firmware upgrade, user management, etc)	1	
Upgradation of the load balancer devices, firmware, patches (as and when released by OEM), softwares and OS as per the organization policies	1	
Installation-reinstallation, configuration and management of HSMs (Network based and PCI based as applicable).	1	

HSM management, administration and monitoring of HSM hardware health, network interfaces and connectivity.	1	
Firmware upgradation, patch management and OEM recommended updates in HSM devices.	1	
Monitoring of HSM performance and security logs.	1	
RCA for HSM & Load Balancer related incidents.	1	
Periodic secure backup of key material and HSM configuration (offline and tamper-proof).	1	
Testing of DR Site HSMs and Load Balancers and ensuring synchronization with primary site.	1	
OEM coordination for hardware replacement and bug fixes.	1	
Support for DR drills as per the drill calendar or as and when needed	1	
Timely closure of the identified vulnerabilities in coordination with the OEM	1	
Proactive monitoring and escalation of incidents	1	
Proactively monitor Load Balancer device health status to detect and report issues	1	
Implement changes, including creation or deletion of VADCs and connectivity setup	1	
Support Switchover and Switchback processes at the Data Centre	1	
Handle complex escalations, including system-wide outages and critical incidents	1	
Provide expertise on change management, ensuring minimal downtime during major updates	1	
Load balancing during EOD and SOD job	1	
Monitoring of CPU, memory, throughput, SSL TPS (transactions per second), session counts, and connection tables.	1	
Application-level performance monitoring (L4 and L7) to detect latency, packet drops, and service degradation.	1	
Allocation of virtual network interfaces, IP addresses, and VLAN bindings.	1	
Resource assignment (CPU, memory, throughput limits) per vADC to ensure optimal load distribution.	1	
Configuration and optimization of supported protocols:	1	
Configuration of appropriate load balancing methods, including but not limited to:	1	
Implementation of persistence/sticky sessions policies (source IP, cookie, SSL session ID, etc.).	1	
URL rewriting and redirection rules.	1	
Compression, caching, and connection multiplexing for performance optimization.	1	
SSL bridging, SSL pass-through, and mutual TLS authentication configuration.	1	
Implementation of access control lists (ACLs), IP restrictions, and rate-limiting policies.	1	
TLS cipher suite optimization to meet industry standards (e.g., disabling weak ciphers).	1	
Integration with Web Application Firewall (WAF) and other security tools where required.	1	
Scheduled configuration backups of all load balancers and vADCs/tenants.	1	
Verification of backup integrity and periodic restoration testing.	1	
Version control of configuration changes with rollback capabilities.	1	
5.5. Storage & Backup Monitoring		
5.5.1. Storage Administration Tasks		
Monitor storage utilization, performance metrics, and capacity trends to ensure optimal resource allocation.	1	
Implement 24×7 monitoring for all storage and backup systems using Bank-approved tools.	1	
Configure alerts for threshold breaches (capacity, performance, job failures, hardware errors) and ensure timely incident resolution.	1	
Maintain real-time dashboards for Bank's visibility into storage and backup health.	1	
Maintain thresholds for proactive scaling before reaching critical utilization levels.	1	
Monitoring of the SAN/NAS devices for availability as per the service window agreed in this SOW	1	
Perform storage user administration	1	
Perform disc quota and rights or permission administration	1	
Coordinate with the hardware vendor for addition, deletion or modification of RAID configuration	1	

Add, delete and modify LUN configuration	1	
Perform physical disk management	1	
Configure, and manage storage and SAN switches	1	
Configuring and managing storage arrays (SAN/NAS)	1	
Configure the SAN Switch for Host Mapping	1	
Perform incident based troubleshooting	1	
Create and map Logical Unit Numbers (LUN) and volumes to different servers based on the inputs provided by the Customer	1	
Manage disk space on LUN	1	
Managing snapshots and replication configurations	1	
Hardware, software and firmware upgrades as and when released by OEM	1	
Creation of Storage Pools and Volume Groups	1	
Reporting to Bank in case of any difference in replication and resolve the same in coordination with OEM & Network Team	1	
Managing complex storage migrations and integrations	1	
Performance tuning and troubleshooting IOPS issues	1	
Advanced performance tuning for high-demand applications	1	
Replication Management [Creation/Modification/Deletion/Monitoring/Synchronization of storage replication]	1	
Troubleshooting vendor-specific storage hardware/software issues	1	
Configure and allocate the required storage capacity based on inputs provided by Customer	1	
LVM Administration	1	
Manage and maintain storage switches and NetApp filers to ensure optimal storage performance and availability.	1	
Configure and administer Storage Area Network (SAN) environments to support data storage and access requirements.	1	
Perform administration and management of file systems, including JFS and JFS2, to ensure efficient storage utilization.	1	
Implement device masking, port settings, and fabric zoning to ensure secure and efficient storage connectivity.	1	
Administer, configure, and maintain all SAN, NAS, and object storage systems, including disk arrays, storage switches, and related components at both DC and DR sites.	1	
Implement storage tiering policies for optimal cost–performance balance.	1	
Maintain high-availability configurations and perform failover testing for storage systems.	1	
Perform quarterly capacity forecasting for storage and backup infrastructure.	1	
Recommend capacity expansion, storage reallocation, and archival strategies to optimize performance and costs.	1	
Identify underutilized storage resources and reclaim them for productive use.	1	
5.5.2. Backup and Restore Management		
Modification to backup policy in consultation with the Customer and adhere to the policy	1	
Modify the backup retention policy in consultation with customer	1	
Provide routine backup and recovery of data with respect to the IT Infrastructure	1	
Periodically monitor the log generated by the backup tool and take appropriate actions	1	
Monitor the performance of scheduled backups, schedule testing of backups as per policy agreed with customer during transition and enable the adherence to related retention policies	1	
Review backup logs to verify successful completion of backup	1	
Notify to customer team any backup failures through automated report, ticket etc	1	
Perform restoration drill as per the schedule agreed with customer during transition and sign off within the limit of available hardware in scope	1	
Management and administration of the Backup software	1	
Verify storage logs and periodically clean up log files	1	

Restricting backup window as per customer specific guidelines	1	
Scheduling and monitoring of OS-level backups.	1	
Restoration testing for OS recovery at regular intervals.	1	
Configuration for OS image backups and bare-metal recovery.	1	
Validate backup integrity through periodic test restores.	1	
Configure, monitor, and administer all enterprise backup systems...	1	
Maintain backup schedules, policies, and retention plans...	1	
Manage offsite backup copies and coordinate secure transport...	1	
Implement data encryption for backups based on the features of the backup solution.	1	
Execution of daily, weekly, and incremental Exchange database backups.	1	
Verification of backup integrity through periodic test restores.	1	
5.6. DR Management		
DR drills will be conducted in scope infrastructure with pre-identified locations and business users participating in a single drill.	1	
Vendor will support the customer in performing switchover and switchback activities as per the defined scope.	1	
Configuration at the Primary Data Center (DC) is to be done by the client unless it is also under the managed scope.	1	
The ISP engaged by the customer will be responsible for ISP-level failover and any changes required for failover to the DR site and back during the DR drill exercise.	1	
The customer must enable business users' systems with the required configuration to access applications from the DR site.	1	
The customer will initiate the DR drill and execute the Business Continuity Plan (BCP).	1	
The customer must provide a minimum of 30 days' advance notice to initiate scheduled DR drills.	1	
DR drill pre-checks must be conducted.	1	
Primary and DR replication must be monitored.	1	
A comprehensive Disaster Recovery Plan (DRP) must be developed, maintained, and updated in alignment with the Bank's BCP.	1	
Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be defined and documented for all critical systems and services.	1	
An updated Application–System–Infrastructure mapping must be maintained to ensure DR readiness.	1	
All production workloads must be validated to have replication or backup mechanisms to the DR site.	1	
Drills must include performance testing of applications post-switch and validation of data integrity after failover and reverse failover.	1	
Detailed drill reports must be documented and submitted.	1	
Coordination with all stakeholders is required to ensure rapid service restoration.	1	
Monthly DR readiness reports must be provided.	1	
Version-controlled DRP documents must be maintained.	1	
Zero data loss beyond the defined RPO must be ensured in all DR events, whether drills or real incidents.	1	
5.7. Other Activities:		
5.7.1. Upgradation & Migration Activities:		
In addition to monitoring, administration and management of DC components, the MSP/Service Provider shall be responsible for carrying out all required upgradation, migration (EOL/EOS assets) in the Bank's Data Centre (DC), Disaster Recovery (DR) Site, and Near DR (if applicable) in a structured, secure, and SLA-bound manner. The activities will include but not be limited to the following:		
Active support for ongoing projects like upgradation / migration of systems to latest supported platforms.	1	
Upgrading end of life Servers, OS, DB and middleware systems.	1	
Validate application compatibility post-patch/upgrade.	1	
Assessment of existing servers, storage, network devices, and security appliances for compatibility with latest versions of firmware, OS, and applications.	1	

Ensuring application compatibility post-upgrade through pre- and post-implementation testing.	1	
Testing, validation, and acceptance sign-off from Bank's application teams before production cutover.	1	
Migration of databases to new hardware or cloud/hybrid environments, as required.	1	
Detailed migration plan with timelines, dependencies, and rollback strategies.	1	
Functional, integration, performance, and security testing after each upgrade/migration.	1	
Please note, Migrations shall be included in the scope for the components that cannot be upgraded due to technical and hosting constraints. Additionally, End-of-Life (EOL) and End-of-Support (EOS) upgrades shall also be the part of the upgrade process. If an application requires a database (DB) or operating system (OS) upgrade, it shall be carried out as part of BAU activities.		
5.7.2. Governance & Escalation Management		
a. Domain Lead (Service Manager)		
The bidder shall designate a DC, DR, NLS Lead and a Domain Lead (Service Manager) for all workstreams. The DC Lead & Service Managers will act as the single point of contact for all service/incident/problem/change-related escalations and must be accessible 24x7 via telephone, email, and web assistance. They will provide support to J&K Users and the CSD team, assisting with problem resolution, addressing concerns and queries, and handling service requests.	1	
The bidder should provide the contact list of DC, DR, NLS leads & domain leads who shall attend to domain-level escalations.	1	
The Bidder shall ensure that an escalation matrix is in place, detailing response timelines and responsible personnel for each escalation level.	1	
b. Governance Framework		
· Establish a joint governance structure between the Bank and the Service Provider for overseeing Data Centre operations, including a steering committee, operational committee, and working groups.	1	
· Prepare and maintain Service Delivery Governance Documents, including governance charter, RACI matrix, and reporting templates.	1	
· Conduct periodic service review meetings at different levels:	1	
o Executive Level – Quarterly review of service performance, risks, and strategic initiatives.	1	
o Operational Level – Monthly review of SLA compliance, incidents, changes, and improvement plans.	1	
o Technical Level – Weekly review of operational issues, tickets, and planned maintenance activities.	1	
· Ensure that governance meetings are minuted, and action items are tracked to closure within agreed timelines.	1	
· Submit governance reports summarizing SLA performance, incident trends, capacity utilization, risk register, and improvement recommendations.	1	
· The MSP shall conduct monthly governance meetings with J&K Bank stakeholders to review SLAs, discuss major incidents, major changes, RCA reports, and improvement plans.	1	
c. Escalation Management		
· Implement a multi-level escalation matrix covering functional, technical, and managerial contacts from both the Bank and the Service Provider.	1	
· Ensure clear definition of escalation triggers such as breach of SLA, prolonged incidents, repeated service failures, or unresolved service requests.	1	
· Maintain round-the-clock availability of escalation contacts for critical and high-severity incidents.	1	
· Escalations must follow a time-bound process:	1	
o Level 1 – Frontline resolution within defined SLA timelines.	1	
o Level 2 – Functional/technical expert involvement within 30–60 minutes of SLA breach or as per incident priority.	1	
o Level 3 – Senior management intervention within 1–2 hours for critical issues.	1	
· Ensure proactive escalation to prevent SLA breaches and minimize business impact.	1	
d. Reporting & Communication		

· Provide incident escalation reports with details of root cause, resolution, and prevention measures.	1	
· Share monthly escalation dashboards highlighting number of escalations, causes, resolution timelines, and recurrence trends.	1	
· Maintain real-time communication with Bank's NOC/IT teams during escalated incidents.	1	
· Ensure that post-resolution, lessons learned are captured and incorporated into SOPs and preventive measures.	1	
e. Continuous Improvement		
· Analyse escalation patterns and recurring issues to identify process gaps and propose corrective actions.	1	
· Recommend automation or process enhancements to reduce escalations.	1	
· Implement service improvement plans (SIPs) with measurable outcomes and agreed timelines.	1	
· Align governance and escalation processes with ITIL best practices and the Bank's internal standards.	1	
5.7.3. Personnel Deployment & Compliance		
a. Personnel Deployment & Training		
· Deploy adequate number of personnel in line with the Bank's approved manpower plan, covering 24x7x365 operations, including weekends and public holidays. Maintain minimum staffing levels at all times.	1	
· Ensure that deployed resources cover all the roles and areas as asked for in this RFP.	1	
· OEM-certified specialists for all domains and technologies as asked for in this RFP. Ensure that all personnel have the required technical certifications, skills, and experience for their assigned roles.	1	
· The Bidder shall ensure that all personnel proposed for deployment at the Bank's site are subject to an interview and approval process by the Bank before onboarding.	1	
· If any appointed personnel are deemed unacceptable by the Bank for any reason, the Bidder shall replace them within one week of receiving such intimation, at no additional cost to the Bank.	1	
· The Bidder shall also provide a suitable backup resource in the absence or leave of the onsite resource(s) to ensure continuity of services.	1	
· The Bidder shall ensure that all deployed personnel adhere to J&K Bank's Supplier IS security policies, Acceptable Usage Policy including background verification (BGV), non-disclosure agreements (NDAs), and cybersecurity training.	1	
· Maintain updated personnel records and provide them to the Bank as and when required.	1	
· Provide refresher trainings and upskilling sessions on new technologies, processes, and tools as per project requirements.	1	
· Conduct familiarization sessions on the Bank's IT policies, security guidelines, and operational procedures before personnel begin work.	1	
· Ensure full compliance with applicable labour laws.	1	
· Ensure timely renewal of labour licenses (if applicable).	1	
· Bear all statutory liabilities related to personnel, including wages, benefits, insurance, and any legal claims.	1	
b. Code of Conduct & Discipline		
· Ensure that all personnel follow the Bank's workplace conduct guidelines, including dress code, behavior, and use of facilities.	1	
· Prohibit use of personal devices in restricted areas unless expressly authorized by the Bank.	1	
· Enforce strict adherence to security protocols, including access control, escort policies, and prohibition on unauthorized data access.	1	
· Replace any personnel whose performance, conduct, or behavior is deemed unsatisfactory by the Bank, within 48 hours of intimation.	1	
c. Continuity & Knowledge Retention		
· Maintain low attrition of deployed staff to ensure operational stability.	1	
· Ensure that departing personnel hand over all access rights, passwords, documents, and assets before release.	1	
· Maintain up-to-date handover/takeover documentation to ensure smooth transition between resources.	1	
d. Audit & Verification		

· Facilitate periodic audits by the Bank or third-party agencies to verify personnel deployment, skill levels, and statutory compliance.	1	
· Provide access to relevant records, including attendance logs, payroll records, training certificates, and compliance documents.	1	
5.7.4. Compliance & Security		
a. Regulatory & Standards Compliance		
· All activities under the scope must be carried out directly by the Bidder's personnel. No activity shall be outsourced or sub-contracted to any third party.	1	
· All configurations, changes, and asset updates must comply with J&K Bank's Supplier IS security Policies, cybersecurity guidelines and regulatory requirements (e.g., RBI, NPCI and applicable regulatory guidelines).	1	
· Small & medium regulatory changes & reports (RBI, Central or State Government, semi-government entities, NPCI) must be implemented without additional commercials, and large regulatory changes & reports as per mutual agreement between the vendor & J&K Bank.	1	
· In case of the contract termination due to regulatory changes, bank and bidder can mutually discuss and agree on the further course of action.	1	
· The vendor shall provide any specific report requested by the Regulator/ Bank / Bank appointed auditors, within the timelines stipulated in the SLA.	1	
· Ensure that governance and escalation processes are auditable with complete activity logs, escalation records, and meeting minutes.	1	
· Maintain compliance with RBI, CERT-In, and other regulatory requirements related to incident and problem management.	1	
· Facilitate internal and external audits related to governance and escalation management processes.	1	
· Periodically review and incorporate regulatory guidelines (e.g., RBI, ISO 22301, ISO 27031) into the DRP.	1	
· Enforce role-based access controls for storage and backup administration.	1	
· Implement audit trails for all configuration changes and administrative actions.	1	
· Ensure compliance with applicable guidelines (RBI, ISO 27001, ISO 22301, etc.) for data protection and backup retention.	1	
· Support regulatory and internal audits by providing logs, reports, and evidence of compliance.	1	
b. Adherence to Information Security guidelines		
· Enforce strong password in line with bank's password policies, multi-factor authentication (MFA), and periodic administrative privilege credential rotation.	1	
· Maintain comprehensive logs of all administrative and privileged activities for at least 1 year or as per Bank's policy.	1	
· Prevent unauthorized physical or logical access to Bank's IT assets.	1	
c. Vulnerability & Patch Management		
· Ensure timely remediation of vulnerabilities as pointed out by the bank's information security team or regulator based on severity:	1	
· Critical – within 24 hours		
· High – within 3 days		
· Medium – within 7 days		
· Low – within 14 days		
· Apply security patches, firmware updates, and hotfixes in accordance with the Bank's change management process.		
d. Data Security & Privacy		
· Ensure encryption of data at rest and in transit as per Bank's policy.	1	
· Restrict copying, transfer, or storage of Bank data outside authorized systems.	1	
· Prevent use of personal storage devices in the DC premises.	1	
· Maintain strict confidentiality of all data	1	
e. Compliance Reporting & Audit Support		
· Provide monthly compliance status reports to the Bank covering regulatory, security, and policy adherence.	1	

· Maintain all evidence of compliance, including logs, access reports, and audit records, for at least 7 years or as per regulatory requirements.	1	
· Facilitate internal, statutory, and third-party audits by providing required documentation, system access, and personnel support.	1	
· Ensure closure of audit findings within the agreed timelines.	1	
f. Continuous Improvement		
· Track industry threats, vulnerabilities, and emerging regulatory requirements, and recommend relevant security enhancements.	1	
· Conduct annual security drills, including disaster recovery, incident response, and breach simulations.	1	
· Provide regular security awareness training for deployed personnel.	1	
5.7.5. Incident, Problem and Change Fulfilment		
Bidder has to follow the Incident management procedure of the bank	1	
Bidder has to provide RCA for all incidents within 24 hours post incident resolution.	1	
The Bidder shall maintain a Knowledge Base documenting common incidents, fixes, and best practices to enhance response efficiency.	1	
The Bidder shall implement automated monitoring & alerting mechanisms to proactively identify issues and reduce incident response time.	1	
The Bidder shall establish a Service Continuity Plan to ensure smooth operations in case of major outages or infrastructure failures.	1	
The Bidder shall be responsible for executing approved changes (pertaining to their respective domains), and all change requests must be fulfilled in accordance with the Bank's approved process, ensuring minimal disruption and adherence to security policies.	1	
The Bidder shall ensure no unauthorized changes are performed and conduct periodic audits to verify compliance with the approved Change Management Process.	1	
5.7.6. Asset & Configuration Management		
The Bidder shall track assets, check quality, and maintain utilization levels, pertaining to their respective domains.	1	
The Bidder shall coordinate with J&K Bank/third-party vendors and perform configuration management accordingly in assets (Assets in Bidder's scope) to incorporate/add new devices/technology implementations.	1	
The Bidder shall perform initial asset verification of all hardware/software and establish the Configuration Management Database (CMDB).	1	
The Bidder shall maintain the asset register and Software Licence Inventory of IT assets inline with Asset Management Procedure and Software Licence Policy of the bank under the scope of DC management, both offline (through Excel) and online (through CMDB), and shall migrate asset records to CMDB as and when needed.	1	
Maintain version-controlled inventory of all hardware, software, and firmware used in storage and backup infrastructure.	1	
The Bidder shall update the asset management database to track all moves, additions, changes, and installations. The physical security of assets will be handled by J&K Bank.	1	
Maintain an up-to-date inventory of all hardware and software assets, including locations, configuration details, serial numbers, asset codes, warranties, and AMC details.	1	
Track licensed software and applications, movement within sites/between locations, and changes in configurations.	1	
Ensure the timely decommissioning of EOL/EOS assets in coordination with J&K Bank, providing recommendations for replacements.	1	
The Bidder shall monitor warranty/AMC details and notify J&K Bank 60 days in advance for contract renewals.	1	
The Bidder should track software/firmware recommendations from OEMs, coordinate hardware/software/firmware upgrades with OEM/vendors, and update the asset database.	1	
The Bidder should track End-of-Life (EOL) and End-of-Support (EOS) statuses of devices and inform/advise J&K Bank accordingly.	1	
5.7.7. Vendor & Third-Party Coordination		

The Bidder shall be responsible for coordinating with OEMs/vendors for software updates, security patches, and firmware upgrades, ensuring minimal downtime.	1	
The selected MSP shall plan, design/re-design, implement, upgrade, operate and optimize all the software, solutions, assets and applications under scope.	1	
The MSP shall also be responsible to operationalize a process to ensure alignment with IT infrastructure and application life cycle management process.	1	
The Bidder shall track and document vendor SLAs, ensuring compliance with service expectations.	1	
Ensure OEM-certified tools and procedures are followed for all changes.	1	
5.7.8. Risk & Audit Reporting		
The Bidder has to provide a risk register on a monthly basis, along with a mitigation plan in a RACI matrix.	1	
The Bidder should have implemented Risk Management policies in their organization and should provide Risk Assessment details to the Bank, including BGV of resources assigned to the Bank.	1	
The Bidder shall establish periodic IT audits, ensuring adherence to J&K Bank's policies and regulatory guidelines.	1	
Conduct annual risk assessment of the DC and DR sites for vulnerabilities (power, cooling, network, security).	1	
5.7.9. Exit & Knowledge Transfer		
a. Exit Management Plan		
· No later than six (6) months prior to contract termination, the Bidder shall conduct comprehensive exit training sessions for the Bank to ensure operational continuity with minimal disruption post-transition. This shall include the complete handover of all relevant documentation, source codes, user guides, and operational insights to the Bank.	1	
· After each training provided to the Bank, the Bidder shall gather participant feedback surveys and conduct knowledge assessments to measure training effectiveness. Any identified gaps or deficiencies shall be promptly addressed through additional training sessions or corrective measures, ensuring alignment with the Bank's operational requirements.	1	
· · Provide quarterly knowledge transfer sessions to the Bank's IT team on storage and backup health, trends, and optimizations.	1	
· Failure to conduct the defined training sessions as per the agreed schedule shall constitute a material breach of contract. The Bank reserves the right to take necessary actions/lay the penalty to address non-compliance.	1	
b. Asset & Configuration Handover		
· Provide a comprehensive asset inventory (hardware, software, licenses, configurations, network diagrams) updated to the last day of service.	1	
· Transfer all original licenses, activation keys, warranty/AMC details, and OEM support contracts related to the Bank's assets.	1	
· Ensure secure handover of all configuration files, scripts, system parameters, and administrative credentials.	1	
· Validate with the Bank's technical team that all systems are functioning as per agreed configurations before the final exit.	1	
c. Documentation Transfer		
· Hand over all Standard Operating Procedures (SOPs), design documents, architecture diagrams, process flows, and incident/problem records.	1	
· Provide detailed records of past upgrades, migrations, changes, and maintenance activities performed during the contract period.	1	
· Submit an updated knowledge repository containing troubleshooting guides, escalation matrices, and vendor contact details.	1	
d. Knowledge Transfer to Bank/Successor		
· Conduct structured knowledge transfer sessions for the Bank's internal teams or incoming service provider covering:	1	
· DC/DR infrastructure layout and dependencies	1	
· System configurations and integrations	1	
· Operational processes, escalation procedures, and monitoring mechanisms	1	

· Ongoing incidents or known issues with resolution status	1	
· Provide hands-on training and shadow-support for a minimum agreed period (e.g., 180 days) post-handover.	1	
· Ensure all knowledge transfer sessions are documented and acknowledged by the Bank.	1	
e. Personnel Transition		
· Ensure continuity of critical staff during the transition period to avoid knowledge gaps.	1	
· Replace any personnel leaving during the exit phase with equally skilled resources without impacting service delivery.	1	
· Facilitate joint working between outgoing and incoming teams for a smooth handover.	1	
f. Data & Access Management		
· Hand over all data, databases, and application repositories in Bank-approved formats.	1	
· Ensure secure deletion/erasure of any Bank data from the Service Provider's devices, systems, or storage media as per Bank policy and provide compliance certificates.	1	
· Revoke all user IDs, passwords, and access privileges to Bank systems, physical premises, and applications held by Service Provider personnel.	1	
g. Compliance & Final Settlement		
· Provide an Exit Completion Report signed by both parties confirming successful transfer and acceptance by the Bank.	1	
· Support audit verification of all exit-related activities. Ensure that all obligations, warranties, and service credits are settled before contract closure.	1	
h. Post-Exit Support (If Applicable)		
· Provide limited-time post-exit support (remote/onsite) as agreed in the contract, to resolve any unforeseen issues arising from the transition.	1	

Note: **Bidders are required to agree to all technical criteria requirements as per the Scope of Work, with**

- A mandatory compliance threshold of **100% for technical parameters.**
- Proposals will be rigorously assessed against these compliance criteria to ensure technical adequacy and alignment with project requirements.

Annexure-F Commercial Bid

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

1. Please be guided by RFP terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.
2. Do not change structure of format nor add any extra items (apart from 4 rows in rate card based scope commercials).
3. 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:

Category	Milestone with Support Required (detailed in the SOW)	Payment Schedule	Total Annual Cost (in Rs.) applicable for 5 Years (Pls provide Per Year Cost)
BAU Activities and Other Deliverables in Scope	All BAU Activities as per scope and domains defined in the RFP delivered at all 3 sites (DC, NLS, DR) of the Bank with Monthly Audit & SLA Compliance	As per Payment terms of RFP	

Indicative Rate Card based Ad-Hoc Project Fee: Based on the tentative scope (Rate card based scope of work- section A point 7), bidder may share the indicative rate card based project fee based on the resources required in the below shown table. (This will not be a part of CQCCBS evaluation, however, rate card shall be used as and when required by the bank). Resources required can include (but will not be limited to) as tabulated below:

1. Migration of Setups (Cloud/Hosted ↔ On-Prem Infrastructure)

Role Category	Level	Daily Rate (Onsite)	Daily Rate (Remote)
Project Manager	L3		
Cloud Architect	L3		
Database Administrator	L2		
Application Specialist	L2		
Security Consultant	L3		
Support Engineer	L2		
Support Engineer	L1		
(Bidder to add based on scope if required)	-		
(Bidder to add based on scope if required)	-		
(Bidder to add based on scope if required)	-		
(Bidder to add based on scope if required)	-		
(Bidder to add based on scope if required)	-		

2. Hyperconverged Infrastructure (Configuration, Maintenance & Support)

Role Category	Level	Daily Rate (Onsite)	Daily Rate (Remote)
HCI Specialist	L3		
Solution Consultant	L3		

Technical Consultant	L3		
Infrastructure Engineer	L2		
Network/Security Engineer	L2		
Support Engineer	L2		
Support Engineer	L1		
(Bidder to add based on scope if required)	-		
(Bidder to add based on scope if required)	-		
(Bidder to add based on scope if required)	-		
(Bidder to add based on scope if required)	-		
(Bidder to add based on scope if required)	-		

Note: Rates to be inclusive of all taxes and other levies but 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.

1. All other Taxes / Duties / levies and charges for packing, forwarding, freight, transit insurance, loading and unloading, shall be borne by bidder.
2. Applicable taxes would be deducted at source, if any, as per prevailing rates.
3. The quantity mentioned above is indicative only and the actual number may change based as per the requirements of the Bank. In case there is any change in the quantity or asset make & model, the same shall be communicated in pre-bid response/corrigendum.

Annexure G: Bank Guarantee Format

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

Offer Reference No.:
Bank Guarantee No: _____
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 India (hereinafter referred to as "Bank" or "J&K Bank") for **Selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)** (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 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 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
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 Bidder has for taken up for **selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)**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 bidder 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 Bidder 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 Bidder 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 Bidder 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 Bidder 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 Bidder 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 Bidder 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 Bidder 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 Bidder

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 Bidder

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

a. Our liability under this Guarantee shall not exceed.....Rupees..... .....only);
b. 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
c. 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.

Dated the..... Day of 2025

For.....

BANK Authorized Signatory

Annexure I: Non-Disclosure Agreement (NDA)

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

THIS NON-DISCLOSURE AGREEMENT (the "Agreement") is made and entered into as of (____/____/2025) 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 **Selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)** 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 of 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/evidence 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 thirty (30) 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: Service Level Agreement (SLA)

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

This Service Level agreement ("Agreement") is made at Srinagar (J&K) on this ……. day of …….2025 ("effective date") between

i. "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 "Successful Bidder" 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:

1) Definitions of the terms

Term	Description
The Bank/J&K Bank	Reference to "the Bank," "Bank," and "Purchaser" shall be determined in context and may mean without limitation "Jammu & Kashmir Bank."
MSP/Bidder/Vendor/Selected Bidder/Company/Service Provider:	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.
PBG	Performance Bank Guarantee.

Data Centre (DC)	Bank's Data Centre located at Noida.
Disaster Recovery (DR)	Bank's 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 not limited to, Information subject to special statutory protection, legal actions, etc.

2) Service Level Management

Service Level Management is the approach Service Provider adopts to monitor, review and report the service level within the Managed IT scope; manages the service in the long run; and embarks on service improvement initiatives.
During Transition, Service Provider will work with J&K bank, to finalize & refine the Service Level Objectives as highlighted in RFP for range of activities under our scope. Service Levels will be applicable post three (3) months on completion of Transition Period.
Service Provider's approach to service management is based on the premise that the service cannot be managed unless it is measured. The key activities in Service Provider's Service Level Management process include as shown in the figure below:

- Identify J&K bank's Service level demands base.
- Define the SLRs (Service Level Requirements) based on J&K bank's business objectives, manage and review them through the Service Lifecycle into Service Quality Plan (SQP) for operational services
- Negotiate, conclude and document the Service Level Agreement
- Monitor and measure service performance achievements of all operational services against targets within service levels
- Produce Service Review Reports
- Conduct Service Review Meeting on a monthly basis, investigate improvements within an overall Service Improvement Plan (SIP).

A. Service Availability

SLA #	SLA Description	Availability	Measurement Period
1	Server & VM Management- (Production- CBS, M-Bank & LOS)	99.9%	Monthly
	Server & VM Management- (Production)	99.5%	Monthly
	Server & VM Management - (Non-Production)	98.5%	Monthly
2	OS & DB Management - (Production- CBS, M-Bank & LOS)	99.9%	Monthly
	Operating System & Database Management- (Production)	99.5%	Monthly
	Operating System & Database Management - (Non-Production)	98.5%	Monthly
3	Middleware Management- (Production- CBS, M-Bank & LOS)	99.9%	Monthly
	Middleware Management- (Production)	99.5%	Monthly
	Middleware Management - (Non-Production)	98.5%	Monthly
4	Load Balancer - (Production- CBS, M-Bank & LOS)	99.9%	Monthly
	Load Balancer- (Production)	99.5%	Monthly
	Load Balancer - (Non-Production)	98.5%	Monthly
5	HSM- (Production- CBS, M-Bank & LOS)	99.9%	Monthly
	HSM- (Production)	99.5%	Monthly

	HSM - (Non-Production)	98.5%	Monthly
6	Backup & Storage - (Production- CBS, M-Bank & LOS)	99.9%	Monthly
	Backup & Storage Management- (Production)	99.5%	Monthly
	Backup & Storage Management- (Non-Production)	98.5%	Monthly
7	DR Management	99.9%	Bi-Annually

For activities including but not limited to: *AD Management, Exchange Mail Messaging, Risk & Audit Reporting, Governance & Escalation Management, Compliance & Security, Onsite Personnel Deployment, Cage Area Monitoring & RMA Coordination, and Vendor/Third-Party Coordination*, - will be governed under the applicable domain-level SLAs or Incident-based SLAs, since any deviation or failure in these activities will result in incident creation, SLA breach, or non-compliance already measurable under existing SLA constructs.

B. Incident Based SLAs

Severity Level	Description	Response Time	Resolution Time	SLA Target
S1	Significant business impact or service outage due to critical component failure, including HA elements, standalone servers, or data centers	10 minutes	01 hours	99%
S2	Non-outage incidents in DC/DR environments, including backup failures or HA-configured server/device issues without service impact.	30 minutes	04 hours	98%
S3	User access, disk utilization, replication, backup, or ISP-related incidents impacting services or non-critical device outages.	60 minutes	08 hours	98%
S4 (Service Requests)	Customer requests for information, user management, disk modifications, backups, or non-break-fix incidents handled per process.	120 minutes	2 Business Days	98%

C. Other Process Based SLAs:

KPI	SLA
Problem Fulfilment	100% RCA Submission within 3 Working Days for Business Impacting Sev-1 Incidents RCA for same asset having repeated S2 incidents will be submitted in 3 to 4 Weeks. This will exclude Capacity Utilization (CPU/Memory/ Disk utilization) related Sev-2 Tickets.
Change Fulfilment	95% successful changes over approved changes in the measurement period
Patch Management	98.00% SLA to be maintained in the measurement period Calculation Metrix: ((Total approved patches -Total patches applied)/Total Patches received) *100
Backup Management	99.00% SLA to be Maintained. Calculation Metrix : (Total no of Backup& Restoration jobs assigned – Backup & Restoration jobs completed/Total number of backup & Restoration jobs) *100
Incident Rate Reduction	5% Incident reduction per quarter basis. Calculation Metric: [(Incidents in Current Quarter-Incidents in Previous Quarter)/Incidents In Previous Quarter)*100)

3) Penalties

The vendor will be contractually obligated to compensate the bank with cash credits if service levels fall below predefined targets, with a maximum penalty of 15% of the quarterly invoice. (Pls note, the below table is for illustrative purposes)

SLA	Measurement Criteria	Weight-age	Points Received based on					Max Score
			1	2	3	4	5	
Severity 1- Resolution	< 01 Hr	15.00%	95.00%	96.00%	97.00%	98.00%	99.00%	0.75
Severity 2- Resolution	< 04 Hrs	10.00%	94.00%	95.00%	96.00%	97.00%	98.00%	0.50
Sev-3 Resolution	<8 Hrs	3.00%	94.00%	95.00%	96.00%	97.00%	98.00%	0.15
Sev-4 Resolution	<2 Business Days	2.00%	94.00%	95.00%	96.00%	97.00%	98.00%	0.10
Server & VM Management- (Production- CBS, M-Bank & LOS)	99.90%	5.00%	99.00%	99.25%	99.50%	99.75%	99.90%	0.25
Server & VM Management- (Production)	99.50%	3.00%	98.00%	98.38%	98.75%	99.13%	99.50%	0.15
Server & VM Management - (Non-Production)	98.50%	2.00%	97.50%	97.75%	98.00%	98.25%	98.50%	0.10
OS & DB Management - (Production- CBS, M-Bank & LOS)	99.90%	5.00%	99.00%	99.25%	99.50%	99.75%	99.90%	0.25
Operating System & Database Management- (Production)	99.50%	3.00%	98.00%	98.38%	98.75%	99.13%	99.50%	0.15
Operating System & Database Management - (Non-Production)	98.50%	2.00%	97.50%	97.75%	98.00%	98.25%	98.50%	0.10
Middleware Management- (Production- CBS, M-Bank & LOS)	99.90%	5.00%	99.00%	99.25%	99.50%	99.75%	99.90%	0.25
Middleware Management- (Production)	99.50%	3.00%	98.00%	98.38%	98.75%	99.13%	99.50%	0.15
Middleware Management - (Non-Production)	98.50%	2.00%	97.50%	97.75%	98.00%	98.25%	98.50%	0.10
Load Balancer - (Production- CBS, M-Bank & LOS)	99.90%	5.00%	99.00%	99.25%	99.50%	99.75%	99.90%	0.25
Load Balancer- (Production)	99.50%	3.00%	98.00%	98.38%	98.75%	99.13%	99.50%	0.15
Load Balancer - (Non-Production)	98.50%	2.00%	97.50%	97.75%	98.00%	98.25%	98.50%	0.10
HSM- (Production- CBS, M-Bank & LOS)	99.90%	5.00%	99.00%	99.25%	99.50%	99.75%	99.90%	0.25
HSM- (Production)	99.50%	3.00%	98.00%	98.38%	98.75%	99.13%	99.50%	0.15
HSM - (Non-Production)	98.50%	2.00%	97.50%	97.75%	98.00%	98.25%	98.50%	0.10
Backup & Storage - (Production- CBS, M-Bank & LOS)	99.90%	5.00%	99.00%	99.25%	99.50%	99.75%	99.90%	0.25
Backup & Storage Management- (Production)	99.50%	3.00%	98.00%	98.38%	98.75%	99.13%	99.50%	0.15
Backup & Storage Management- (Non-Production)	98.50%	5.00%	97.50%	97.75%	98.00%	98.25%	98.50%	0.25
DR Management	99.90%	3.00%	99.00%	99.25%	99.50%	99.75%	99.90%	0.15
Problem Fulfilment	100.00%	1.00%	90.00%	92.50%	95.00%	97.50%	100.00%	0.05
Change Fulfilment	95.00%	1.00%	85.00%	87.50%	90.00%	92.50%	95.00%	0.05
Patch Management	98.00%	0.50%	90.00%	92.00%	94.00%	96.00%	98.00%	0.03
Backup Management	99.00%	0.50%	98%	98.25%	98.50%	98.75%	99.00%	0.03
Incident Rate Reduction	5.00%	0.50%	1.00%	2.00%	3.00%	4.00%	5.00%	0.03
Reporting & Governance	100.00%	0.50%	4 missed	3 missed	2 missed	1 missed	0 missed	0.03
		100%						5.00

SLA Scoring (out of 5)	Penalty
>4.5	0%
>4 to <=4.5	2.50%
>3 to <=4	5.00%
3	7.50%
<3 to >=2	10.00%
<2 to >=1.5	12.25%
<1.5	15%

The selected bidder shall be required to comply with all Service Level Agreements (SLAs) as defined in this RFP and the subsequent contract. In the event of any deviation from the agreed SLA thresholds, the Bank shall impose penalties in a structured and proportionate manner.
In case of repeated breaches or non-adherence to SLA compliance, the Bank reserves the right to impose additional penalties of up to 3%, or initiate a performance review and take action as per the contract's exit/termination clause.

4) Other Penalties / Liquidated Damages

- Non-compliance on start of project/support as per project milestones from the date of the acceptance of the Bank's Purchase Order will result in termination of contract and revoking/cancellation of P.O.
- Failure to comply with governance processes, including timely submission of reports, participation in review meetings, and adherence to PMO requirements, shall attract penalties as defined in the Contract.
- Exit Management & Knowledge transfer: Non-fulfilment of exit management obligations, including knowledge transfer, documentation, and exit training as stipulated in the Contract, shall attract penalties to ensure smooth transition without disruption to services.
- The liquidated damages shall be deducted / recovered by J&K BANK from any money due or becoming due to the Bidder under this purchase contract or may be recovered from bidder or from any other pending/amount payable to the bidder in respect of other Orders without prejudice to
- J&K BANK's right to levy any other penalty where provided for under the contract.

- All the above LDs are independent of each other and are applicable separately and concurrently. However the total Liquidated Damages to be recovered under any clause shall be restricted to 10% of the total value of the payments due for the quarter.
- LD is not applicable for reasons attributable to J&K BANK and Force Majeure. However, it is the responsibility/onus of the Bidder to prove that the delay is attributed to J&K BANK and Force Majeure.
- The Bidder shall submit the proof authenticated by the Bidder and J&K BANK's official that the delay is attributed to J&K BANK and/or Force Majeure at the time of requesting installation payment. If the Bidder fails to produce proof of delay on the part of J&K BANK's officials that in turn caused delay in installation, if any, the date of installation shall be taken for calculating the delay for LD purpose.
- J&K BANK reserves the right to impose / waive/ reduce any such penalty.

5) Governance & Reporting

The Successful Bidder shall ensure adherence to the timelines defined in the table below during the contract period:

Deliverable	Target	Remarks
Daily Status Report	By 11AM of the next working day	Failure to submit for 3 consecutive dates will attract a review
Weekly Status Report	By 11AM of first working day of the following week	Failure to submit for 3 consecutive dates will attract a review
Monthly Status Report	By the 10th of the next month	Failure to submit for 3 consecutive dates will attract a review
As & when required – Report requested by the Regulator/ Bank / Bank appointed auditors (as and when required)	Within 12 hours from the time the request is made to the Vendor	Failure which will attract a review

The monthly reports as required to be submitted by the bidder to carry the Governance & Reporting meetings shall broadly include, but shall not be limited to below:

- Server/Asset wise uptime/downtime reports
- Incident and Change Management/Fulfilment Request Reports
- RCA reports
- Risk & Audit Reports
- Compliance reports
- SLA breach reports
- Upgrade & Migration reports
- Asset wise Patching report mentioning the current patch set (and OS/DB/WLS version) in the setups
- VAPT Closure reports
- Backup failure reports
- DR Drill reports
- Cage Area Monitoring and Logs
- RMA (carried by AMC Vendor) and post RMA Server Asset functioning reports.
- CPU, RAM, Storage utilization/breach reports.
- Asset & Configuration Management
- Onsite Personnel Deployment & Compliance

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 /PBG

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.

6) Contract Period

The tenure of the Contract will be for a period of 5 years, effective from acceptance of Purchase Order /successful go live i.e. _____ till _____, unless or until terminated by Bank in accordance with the terms of this SLA. The contract may be extended for a further period at mutually agreed terms and conditions.

7) Payment Terms

Category	Description	Payment Payout w.r.t Total TCV Amount	Billing Frequency	Penalty Applicability
Contract Signing & Project Kick-off	Payment post Signing the contract, Initial planning and assessment along with mobilization/ deployment of resources	**5%**	One Time	Not Applicable
Mobilization of Resources	Deployment of all required qualified personnel at DC, NLS, DR, as per resource qualification & experience years criteria shown in the RFP (Post interview by Bank Team wherever required)	**5%**	One Time	SLA-linked penalty on domain fee
Service Commencement / Go-Live at all 3 sites (DC, NLS, DR) along with base Audit Completion and Starting of all BAU Activities (as defined in the RFP) with Monthly SLA Compliance	Upon Successful start of SLA-Based BAU operations including servers, storages, databases, application administration, BCP Activities, Backup shipping /restoration etc. Linked to SLA Performance: Uptime, incident response, change management, patching, backup success, storage performance, monitoring and reporting.	**90%**	**Quarterly in Arrears** post Governance & review meetings with Bank on SLA adherence, incidents, RACs, Upgrades, hardening, Patching, VAPT Closures etc. Detailed Reports to be submitted to the Bank in support of Uptime commitments against each BAU Activity separately.	SLA-linked penalty on domain fee
Rate Card for Ad-Hoc Projects	Cloud to On-Prem - Major migration projects Hyperconverged Infrastructure deployment and configuration	Per Project Mutually agreed between bank and MSP	Based on Mutual Agreement	NA

Table 8: Payment Schedule

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

- No advance payment will be made on award of the contract.
- Quarterly in arrears on submission of invoices and preventive maintenance reports duly signed by the official of the concerned after deduction of charges / Liquidated damages (if any) mentioned in the agreement.
- All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.
- Payments will be withheld in case of Non-compliance of the terms and condition of this RFP.

Payments shall be released on acceptance of the purchase order and:

e. Post Signing of Service Level Agreement (SLA) between Bank and Successful bidder.
f. Post Signing of Non-Disclosure Agreement (NDA) between Bank and Successful bidder.
g. All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.
h. No Payment shall be made for the transaction processed beyond the timelines.

8) Assignment

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

9) 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.

10) 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.

11) 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.

12) Partnership / Collaboration / Subcontracting

The services offered shall be undertaken to be provided by the company directly and there shall not be any sub-contracting. L1, L2 & L3 resources shall be strictly on bidder's payroll. L1 Technical Support, if necessary, however can be taken from Authorized Service Delivery Partners for not more than 20% with prior approvals from the Bank Team, however in such a case also, the overall SLA ownership shall remain with the bidder only. Bank will only discuss the solution with company's own 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 bidder 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 Successful Bidder without prior written consent of the Bank.

13) 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.

14) Information security

(a) The Successful 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 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:

  (i) Ensure the security and confidentiality of Customer Data, Protect against any anticipated threats or hazards to the security or integrity of Customer Data

  (ii) 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. Successful Bidder shall comply with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data.

(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 be 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) Successful Bidder's criticality assessment shall be conducted for all partners & vendors. Appropriate management and assurance on security risks in outsources and partner arrangements shall be ensured.

15) 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 six months prior notice.

In the event of termination of the Agreement for the Bank's convenience, Successful Bidder 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.

16) 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 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.

17) Right to Audit

Bank reserves the right to conduct an audit/ ongoing audit of the services provided by Bidder.

The Selected Bidder shall be subject to annual audit by internal/ external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India 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 Successful Bidder is required to submit such certification by such Auditors to the Bank.

Bidder should allow the J&K Bank or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Bidder 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. Bidder should allow the J&K 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.

18) 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 Successful Bidder, under this agreement shall not exceed total contract value.

19) 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) Serious 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 Successful Bidder. Bank reserves right to exit at any time after giving notice period of 60 days during the contract period.

20) 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, 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 bidder r 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 Successful Bidder 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

21) Intellectual Property Rights

i. For any technology / software / product used by Company for performing Services for the 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.

ii. 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.

iii. 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.

iv. 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 Of successful bidder

v. 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.

22) 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.

23) 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 Successful 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 **DC-DR Monitoring & Management Services** and designated representative of the Successful Bidder. If designated Officer of the Bank and representative of the Successful 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 the Successful Bidder respectively. If even after elapse of reasonable period, which in any case shall not exceed 60 days, the senior authorized personnel designated by the Bank and the Successful Bidder 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 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.

24) 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:

General Manager (S&IT), J&K Bank Ltd,

Technology & Development Division,

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

Following shall be address of Company for notice purpose:

_____

_____

_____

25) Other Terms and Conditions

All eligibility requirements mentioned in Annexure -D should be complied by the bidders as applicable and relevant support documents should be submitted for the fulfilment of eligibility criteria failing which the Bids may be summarily rejected. Noncompliance of any of the criteria can entail rejection of the offer. Copies of relevant documents / certificates should be submitted as proof in support of the claims made for each of the above-mentioned criteria and as and when the bank decides, originals / certified copies should be shown for verification purpose. J&K Bank reserves the right to verify / evaluate the claims made by the Bidder independently. Any deliberate misrepresentation will entail rejection of the bid/proposal.

1. 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.

2. 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.
3. 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.
4. Any addition, alteration, amendment, of this Agreement shall be in writing, signed by both the parties.
5. 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.
6. 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.
7. 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……

Annexure K: Undertaking

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

To
The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank MA Road, Srinagar

Dear Sir,

Sub: RFP No …….. For selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR), dated …… 2025

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide **selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)** for J&K Bank 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 hereby undertake that supporting software/license supplied, if required will be licensed, legally obtained and with latest version.

We understand that the Bank is not bound to accept the offer either in part or in full and that the Bank has right to reject the RFP in full or in part without assigning any reasons whatsoever.

We have read, understood and accepted the terms/ conditions/ rules mentioned in the RFP including the conditions applicable to CQCBS 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.

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/- (Rupees Five Thousand Only) and EMD of Rs.1,00,00,000/- (Rupees One Crore 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 _____2025

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.

Place:

Seal and signature of The Bidder

Annexure L: Know Your Employee

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

To
The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank MA Road, Srinagar

Dear Sir,

Sub: RFP No …….. For selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR), dated …… 2025

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.. **selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)** for J&K Bank 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 DC-DR Monitoring & Management Services for J&K Bank.

Note: These details should be on the letterhead of the bidder company and each & every page should be signed by their Authorized Signatory with name and seal of the company.

Place:
Date:

Seal and signature of the bidder

Annexure M: No Deviation Certificate

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

To
The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank MA Road, Srinagar

Dear Sir,

This is to certify that our offer is exactly in line with your RFP for **selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR)** No._____ dated _____ and subsequent corrigenda's. This is to expressly certify that our offer contains no deviation either Technical or Commercial in either direct or indirect form.

Date:

Name and Designation of Signatory:

Name of Company:

Address:

Note: This form must be signed by authorized signatory.

Annexure N: Reference Site Details

(To be submitted under the letter head of the bidder company and signed by Authorized Signatory)

To
The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank MA Road, Srinagar

Bidder shall provide the necessary number of referenced for fulfilling the eligibility criteria. Please provide reference details in the format defined below and enclose the necessary documentary proof:

S.N.	Particulars		Bidder's Response
1.	Name of Organization (Client)		
2.	No. of Branches/offices		
3.	Address of organization		
4.	Date of PO		
5.	Contract Duration	From	
		To	
6	Contract Value		
6.	Status (Completed/ In Progress)		
7.	Brief details of scope of work		
8.	Order Quantity Supplied	Manpower L1	
		Manpower L2	
		Manpower L3	
		Admin Level Resources	
9.	Name of contact person in-charge from client side for reference		
10.	Contact no. of contact person from client side		
11.	Email ID of contact person from client side		

The reference sites submitted must be necessarily of those banks/companies where bidder has been awarded the contract prior to date of issuance of this RFP.
For those references where the offered delivery is accepted but installation is not started, the acceptance should be valid as on the last date of submission of bids at J&K Bank.

Note: These details should be on the letterhead of the bidder company and each & every page should be signed by their Authorized Signatory with name and seal of the company.

Place:

Date:

Seal and signature of the bidder

Annexure O: Undertaking of Vendor Resource Expertise

To be submitted under the letter head of the bidder company and signed by Authorized Signatory

To
The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank MA Road, Srinagar

Dear Sir,

Sub: RFP No …….. for selection of vendor to provide SLA-bound Data Centre Management Services to the Bank for all its infrastructure components and services hosted in its Primary Data Centre (DC), Near Line Site and Disaster Recovery Site (DR), dated …… 2025

The Vendor affirms that these tables represent the minimum requirements. All deployed personnel will meet these criteria or higher. Any deviation must be approved in writing by the Bank in advance.

Resource Qualification Criteria
The selected Service Provider shall deploy resources with the qualifications, certifications, and experience necessary to manage the Bank's Data Centre (DC), Disaster Recovery (DR) and Near Line sites in line with the scope of work, SLA obligations, and regulatory compliance requirements.

General Requirements for All Deployed Personnel

- All deployed personnel shall be full-time employees of the Service Provider. However, if necessary, not more than 20% L1 resources from Authorized Service Delivery Partners shall be allowed with prior approvals from the Bank Team, however in such a case also, the overall SLA ownership shall remain with the bidder only.
- All resources must be background-verified (police verification, previous employment, and education verification).
- All resources must comply with the Bank's Information Security & Confidentiality Guidelines.
- All resources shall be physically deployed on-site at the DC/NLS/DR as per the shift roster approved by the Bank.
- All resources must have good communication skills in English and Hindi.
- Shift coverage must be 24x7x365 with adequate overlap for handover.
- Not more than 25 resources would be deployed in a shift by the MSP, as per the shift schedule intimated to the Bank.

Qualifications & Experience Matrix (L1 / L2 / L3)

The bidder must ensure that all proposed team members (L1/L2/L3) meet the following minimum qualification, experience requirements and below shown OEM Certifications for Data Center management:

1. DC Manager / Project Lead minimum 7+ years in DC operations with at least 3-4 years in a managerial role leading a team of 10 people or more in DC Operations.
2. L1 Support: Minimum 2-3 years of relevant experience
3. L2 Support: Minimum 4-5 years of relevant experience
4. L3 Support: Minimum 6-7 years of relevant experience

Domain	Technology / Platform	At least 70% of L1 Resource Qualification	At least 70% of L2 Resource Qualification	At 70% of L3 Resource Qualification
Operating Systems	Windows / Linux / Unix	Graduate with Diploma in IT/ BE/B.Tech/ MCA /B.Sc./ME/MSc	BE/B.Tech/M.Tech/MCA/B.Sc./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ME/MSc and equivalent qualifications

		and equivalent qualifications		
Databases	Oracle DB, MS SQL, MySQL, PostgreSQL, MongoDB, IBM Db2, SAP HANA, Exadata/ExaCC	Graduate with Diploma in IT/ BE/B.Tech/ MCA /B.Sc./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ME/MSc and equivalent qualifications
Middleware	WebLogic, JBoss, Apache, WebSphere, TIBCO	Graduate with Diploma in IT/ BE/B.Tech/ MCA /B.Sc./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications
Virtualization	VMware, OCI, OCP, OKE	Graduate with Diploma in IT/ BE/B.Tech/ MCA /B.Sc./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications
Storage	Hitachi VSP, Dell EMC, NetApp, HPE, IBM	Graduate with Diploma in IT/ BE/B.Tech/ MCA /B.Sc./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications
Backup & DR	Commvault, Veeam, Dell EMC Data Domain, DP	Graduate with Diploma in IT/ BE/B.Tech/ MCA /B.Sc./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications	BE/B.Tech/M.Tech/MCA/B.Sc./ ./ME/MSc and equivalent qualifications

Role-wise OEM Certification for L1, L2 and L3 Resources on each Matrix (OS, DB, Middleware, Virtualization, Cloud, Storage & Backup)

Domain	Technology / Platform	At least 60% of L1 (Entry / Associate)	At least 60% of L2 (Intermediate / Professional)	At least 60% of L3 (Advanced / Expert)
Server	Microsoft Windows Server / Azure	Azure Fundamentals (AZ-900), Microsoft 365 Fundamentals (MS-900), Security & Compliance Fundamentals (SC-900)	Azure Administrator Associate (AZ-104), Microsoft 365 Administrator Associate	Azure Solutions Architect Expert (AZ-305), Microsoft Certified: Cybersecurity Architect Expert
	Linux (Red Hat)	Red Hat Certified System Administrator (RHCSA – EX200)	Red Hat Certified Engineer (RHCE – EX294)	Red Hat Certified Architect (RHCA)
	Linux (SUSE)	SUSE Certified Administrator (SCA)	SUSE Certified Engineer (SCE)	SUSE Certified Architect
	Linux (Ubuntu / Canonical)	Ubuntu Certified Associate	Ubuntu Certified Professional	Ubuntu Advanced Administrator (Canonical training)
	Oracle Solaris	Oracle Solaris 11 System Administrator Certified Associate	Oracle Solaris 11 System Administrator Certified Professional	Oracle Solaris 11 System Administrator Certified Implementation Specialist
	IBM AIX	IBM Certified Administrator – AIX	IBM Certified Advanced Technical Expert – AIX	IBM Certified Solution Architect – AIX
	HP-UX	HPE Accredited Technical Professional (ATP) – HP-UX	HPE ASE – HP-UX Advanced Admin	HPE Master ASE – HP-UX & Virtualization

Databases	Microsoft SQL Server	Azure Data Fundamentals (DP-900), SQL Server Database Fundamentals (legacy MTA)	Azure Database Administrator Associate (DP-300)	Azure Solutions Architect Expert / Data Engineer Expert
	Oracle DB	Oracle DB OCA	Oracle DB OCP	Oracle DB OCM
	MySQL	MySQL Database Administrator OCA, MySQL Developer OCA	MySQL Database Administrator OCP, MySQL Developer OCP	MySQL Database Administrator Certified Professional / Specialist
	PostgreSQL	EDB Certified Associate (Postgres)	EDB Certified Professional	EDB Certified Advanced Architect
	MongoDB	MongoDB Certified DBA Associate	MongoDB Certified DBA Professional	MongoDB Certified Architect
	IBM Db2	IBM Certified Database Associate – Db2	IBM Certified Database Admin – Db2	IBM Certified Advanced Database Admin – Db2
	SAP HANA	SAP Certified Technology Associate – HANA	SAP Certified Technology Specialist – HANA	SAP Certified Technology Professional – HANA
	Oracle Exadata / ExaCC	Exadata/CC Database Machine Administrator Associate	Exadata/CC Database Machine Admin Professional	Exadata/CC Certified Implementation Specialist
Middleware	Oracle WebLogic	WebLogic Server Certified Associate	WebLogic Certified Implementation Specialist	WebLogic Certified Expert / Specialist
	Red Hat JBoss EAP	RH Certified Specialist in JBoss EAP	RH Certified Specialist in JBoss Admin	RHCA (with JBoss specialty)
	Apache Tomcat	Apache Tomcat Admin Basics	Apache Tomcat Advanced Administrator	Apache Middleware Architect
	IBM WebSphere	IBM Certified Admin – WebSphere ND	IBM Certified SysAdmin – WebSphere ND	IBM Certified Solution Architect – WebSphere
	Oracle Fusion Middleware / SOA	SOA Suite Certified Associate	SOA Suite Certified Implementation Specialist	Fusion Middleware Certified Expert
	TIBCO	TIBCO Messaging Associate	TIBCO Certified Professional	TIBCO Certified Architect
Virtualization & Cloud	VMware	VMware Certified Technical Associate (VCTA – DCV, NV, CMA, DTM)	VMware Certified Professional (VCP – DCV, NV, CMA, DTM)	VMware Certified Advanced Professional (VCAP) / VMware Certified Design Expert (VCDX)
	Oracle Cloud (OCI)	OCI Foundations Associate (1Z0-1085)	OCI Architect Associate (1Z0-1072)	OCI Architect Professional (1Z0-997)
	Kubernetes / Containers (Red Hat OCP)	RH Specialist in Containers & Kubernetes (EX180)	RH OpenShift Administrator (EX280)	RH OpenShift Architect (multiple specialist tracks)
	Oracle Kubernetes Engine (OKE)	OCI Kubernetes Engine Specialist (Learning Path)	OKE Implementation Specialist	OCI Cloud Native Architect
Storage & Backup	Hitachi VSP	Hitachi Vantara Storage Foundations / Associate	Hitachi Certified Specialist – Storage Administration	Hitachi Certified Expert – VSP / Solutions Architect
	Dell EMC	Dell EMC Proven Professional Associate	Dell EMC Specialist – Storage Admin	Dell EMC Expert – Storage Architect
	NetApp	NetApp Certified Storage Associate (NCSA)	NetApp Certified Data Administrator (NCDA)	NetApp Certified Implementation Engineer / Architect (NCIE / NCDAE)

	HPE Storage	HPE ATP – Storage Solutions	HPE ASE – Storage Solutions Architect	HPE Master ASE – Storage Solutions
	IBM Storage	IBM Certified Specialist – Storage Solutions	IBM Certified Advanced Storage Specialist	IBM Certified Storage Solution Architect
	Commvault	Commvault Certified Professional – Fundamentals	Commvault Certified Professional – Specialist / Advanced	Commvault Certified Master / Expert
	Veritas NetBackup	Veritas NetBackup Associate	NetBackup Professional / Specialist	NetBackup Expert / Architect
	Veeam	Veeam Certified Engineer (VMCE) Associate	VMCE Professional	VMCE Expert / Architect
	Dell EMC Data Protection	Associate – Data Protection and Management	Specialist – Data Protection	Expert – Data Protection Solutions

Additional Compliance Conditions

1. Resource Replacement: Any replacement resource must meet or exceed the above qualifications/certification and experience and must be approved by the Bank before deployment.
2. Continuous Training: Service Provider shall ensure all deployed resources undergo periodic refresher training in ITIL processes, security best practices, and OEM technology updates.
3. Performance Review: The Bank reserves the right to review individual resource performance and request replacement in case of underperformance or SLA breach.

Place:

Date:

Seal and signature of the bidder