



**Online Request for Proposal (e-RFP)  
For**

**Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model**

**e-RFP Ref.No.JKB/CHQ/T&D/SSP-UPI-JKB/2025-1468  
Dated : 18-07-2025**

Issued By  
J&K Bank  
Technology & Development,  
Fifth Floor, Corporate Headquarters  
MA Road, Srinagar  
Phone No : +91- 9596197798  
Email id: junaid.mattoo@jkbmail.com

## SCHEDULE OF RFP

|  |   |
|--|---|
| e-RFP Reference No.  | JKB/CHQ/T&D/SSP-UPI-JKB/2025-1468<br>Dated : 18-07-2025   |
| Date of Issue of e-RFP   | 21-07-2025  |
| e-RFP Description  | Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model  |
| Issuer of the RFP-Department   | Technology & Development Department   |
| Bank's Communication Details   | J&K Bank<br>Technology & Development,<br>5th Floor, Corporate Headquarters, MA Road,<br>Srinagar<br>Mr. Junaid Riaz Mattoo<br>Phone No : +91- 9596197798<br>Email id:- Junaid.mattoo@jkbmail.com  |
| RFP Application Fee<br>(Non - Refundable )   | Rs.2,500/- (Rupees Two Thousand Five Hundred Only) to be deposited through Transfer / NEFT to the below detailed A/c:<br>Account Name: <b>Tender Fee/ Cost Account</b><br>16-digit Account No : <b>9931530300000001</b><br>IFSC Code: JAKA0HRDCHQ (0 denotes zero)<br>Bank: The J&K Bank Ltd<br>Branch: Corporate Headquarters  |
| Earnest Money Deposit ( EMD)(<br>Refundable )  | Rs.70,00,000/- (Rupees Seventy Lac Only) to be deposited through transfer / NEFT to the following A/c with Bank details given as:<br>Account Name: <b>Earnest Money Deposit(EMD)</b><br>16-digit Account No : <b>9931070690000001</b><br>IFSC Code: JAKA0HRDCHQ (0 denotes zero)<br>Bank: The J&K Bank Ltd<br>Branch: Corporate Headquarters<br>MA Road Srinagar J&K - 190001 |
| Performance Bank Guarantee   | 5% of total contract Value  |
| Bid Document Availability<br>including<br>changes/amendments, if any<br>to be issued | RFP may be downloaded from<br><a href="https://jkbank.abcpocure.com">https://jkbank.abcpocure.com</a> from:<br>July 21, 2025 16.00 Hrs to<br>August 11, 2025 17.00 Hrs.   |

| Last date for pre-Bids queries & submission Mode | on-line through the prescribed e-Tendering portal<br><a href="https://jkbank.abcpocure.com">https://jkbank.abcpocure.com</a><br>Up to July 29, 2025 17.00 Hrs.   |        |      |   |                               |   |                          |   |                                 |   |                            |
|--|--|--------|------|---|-------------------------------|---|--------------------------|---|---------------------------------|---|----------------------------|
| Pre-bid Queries Response date                    | All communications regarding points / queries requiring clarifications shall be given online on<br>Up to August 04, 2025 17.00 Hrs.  |        |      |   |                               |   |                          |   |                                 |   |                            |
| Last Date of Submission of RFP Bid               | August 11, 2025 17.00 Hrs.   |        |      |   |                               |   |                          |   |                                 |   |                            |
| Submission of online Bids                        | As prescribed in Bank's online tender portal<br><a href="https://jkbank.abcpocure.com">https://jkbank.abcpocure.com</a>  |        |      |   |                               |   |                          |   |                                 |   |                            |
| Date and time of opening of technical bid        | To be notified separately  |        |      |   |                               |   |                          |   |                                 |   |                            |
| Corrigendum                                      | All the Corrigendum will be uploaded on online tender portal<br><a href="https://jkbank.abcpocure.com">https://jkbank.abcpocure.com</a> only   |        |      |   |                               |   |                          |   |                                 |   |                            |
| For e-Tender related Queries                     | <p><b>Service Provider:</b></p> <p>M/s. E-procurement Technologies Limited<br/>( Auction Tiger) , B-705, Wall Street- II, Opp. Orient Club, Ellis Bridge,<br/>Near Gujarat College,<br/>Ahmedabad- 380006, Gujarat</p> <p><b>Help Desk:</b></p> <table border="1"> <thead> <tr> <th>Sr. No</th><th>Name</th></tr> </thead> <tbody> <tr> <td>1</td><td>Sandhya Vekariya – 6352631968</td></tr> <tr> <td>2</td><td>Suraj Gupta – 6352632310</td></tr> <tr> <td>3</td><td>Ijlalaehmad Pathan – 6352631902</td></tr> <tr> <td>4</td><td>Imran Sodagar - 9328931942</td></tr> </tbody> </table> | Sr. No | Name | 1 | Sandhya Vekariya – 6352631968 | 2 | Suraj Gupta – 6352632310 | 3 | Ijlalaehmad Pathan – 6352631902 | 4 | Imran Sodagar - 9328931942 |
| 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               |
| PO   | Purchase Order                  |
| RFP  | Request For Proposal            |
| AMC  | Annual Maintenance Contract     |
| UPI  | Unified Payment Interface       |
| IMPS | Immediate payment service       |





## CONTENTS

| <u>SECTION A-INTRODUCTION</u> |                                      |   |   |
|-------------------------------|--------------------------------------|---|---|
| 1                             | <a href="#">Brief about Bank</a>     | 5 | <a href="#">Broad Scope of Work</a>         |
| 2                             | <a href="#">Purpose Of RFP</a>       | 6 | <a href="#">Location of Work</a>            |
| 3                             | <a href="#">Eligibility Criteria</a> | 7 | <a href="#">Invitation for Tender Offer</a> |
| 4                             | <a href="#">Brief Scope of Work</a>  | 8 | <a href="#">Project Delivery Milestones</a> |

| <u>SECTION B-EVALUATION PROCESS</u> |   |   |  |
|-------------------------------------|---|---|--|
| 1                                   | <a href="#">Stage A-Evaluation of Eligibility</a>   | 3 | <a href="#">Stage C-Evaluation of Commercial Bid</a> |
| 2                                   | <a href="#">Stage B-Evaluation of Technical Bid</a> |   |  |

| <u>SECTION C-RFP SUBMISSION</u> |  |    |   |
|---------------------------------|--|----|---|
| 1                               | <a href="#">e-tendering Process</a>        | 8  | <a href="#">Deadline for Submission of Bids</a>     |
| 2                               | <a href="#">Service Provider</a>           | 9  | <a href="#">Bid Validity Period</a>                 |
| 3                               | <a href="#">RFP Fees</a>                   | 10 | <a href="#">Bid Integrity</a>                       |
| 4                               | <a href="#">Earnest Money Deposit</a>      | 11 | <a href="#">Cost of Bid Document</a>                |
| 5                               | <a href="#">Performance Bank Guarantee</a> | 12 | <a href="#">Contents of Bid Document</a>            |
| 6                               | <a href="#">Tender Process</a>             | 13 | <a href="#">Modification and Withdrawal of Bids</a> |
| 7                               | <a href="#">Bidding Process</a>            | 14 | <a href="#">Payment Terms</a>                       |

| <u>SECTION D-GENERAL TERMS &amp; CONDITIONS</u> |   |    |   |
|---|---|----|---|
| 1   | <a href="#">Standard of Performance</a> | 16 | <a href="#">No Agency</a>               |
| 2   | <a href="#">Indemnity</a>               | 17 | <a href="#">Project Risk Management</a> |

|    |  |    |  |
|----|--|----|--|
| 3  | Cancellation of Contract and Compensation                                  | 18 | Information Security                       |
| 4  | Liquidated Damages   | 19 | No Set-Off, Counter-Claim and Cross Claims |
| 5  | Fixed Price  | 20 | Statutory Requirements                     |
| 6  | Right to Audit   | 21 | Bidder Utilization of Know-how             |
| 7  | Force Majeure  | 22 | Corrupt & Fraudulent Practices             |
| 8  | Publicity  | 23 | Solicitation of Employees                  |
| 9  | Amendments   | 24 | Proposal Process Management                |
| 10 | Assignment   | 25 | Confidentiality Provision                  |
| 11 | Applicable law and jurisdictions of court                                  | 26 | Sub-Contracting                            |
| 12 | Resolution of Disputes and Arbitration clause                              | 27 | Reverse Auction                            |
| 13 | Execution of Service Level Agreement (SLA)/ Non-Disclosure Agreement (NDA) | 28 | Award Notification                         |
| 14 | NO CLAIM Certificate   | 29 | Suspension of Work                         |
| 15 | Cost And Currency  | 30 | Taxes & Duties                             |

#### SECTION E-Annexures

|   |   |    |   |
|---|---|----|---|
| 1 | Annexure A-Confirmation of Terms and Conditions       | 9  | Annexure G: Bank Guarantee Format             |
| 2 | Annexure B: Tender Offer Cover Letter                 | 10 | Annexure H: Performance Bank Guarantee Format |
| 3 | Annexure C: Details of Bidder                         | 11 | Annexure I: Non-disclosure Agreement (NDA)    |
| 4 | Annexure D and D1: Compliance to Eligibility Criteria | 12 | Annexure J: Service Level Agreement           |

|   |   |    |  |
|---|---|----|--|
| 5 | <a href="#">Annexure E: Technical Bid Format</a>      | 13 | <a href="#">Annexure K: Undertaking</a>                  |
| 6 | <a href="#">Annexure E1:Technical Specifications</a>  | 14 | <a href="#">Annexure L: Know Your Employee</a>           |
| 7 | <a href="#">Annexure E2:Functional Specifications</a> | 15 | <a href="#">Annexure M:Compliance Requirements</a>       |
| 8 | <a href="#">Annexure F: Commercial Bid Format</a>     | 16 | <a href="#">Annexure N: Hosting Assessment Checklist</a> |

## 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. Bank is listed on the NSE and the BSE and has its Corporate Headquarters at Srinagar. 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. Further details of Bank including profile, products and services are available on Bank's website at <https://www.jkbank.com>

### 2. Objectives of the RFP

J&K Bank through this RFP process seeks a detailed technical & commercial proposal to onboard a reputed Service Provider with proven experience in the field of providing end-to-end UPI/IMPS) Solution on hosted model (OPEX) Model. In this endeavor, the Bank invites proposals from capable and experienced Bidders to provide a comprehensive solution & an agreement would be entered into with the successful bidder for a period of three years extendable by two years

Successful Bidder shall deploy Application setup on DC & DR on Private Cloud of the Bidder for Bank. The Bidder will be responsible for routing, processing, validation, reporting etc. the transaction to and from NPCI, originated from the Switch/Bank's/other various alternative channels which is used by its customers.

The bidder shall be responsible for providing, implementation & maintenance of the solution throughout the contract period

The bidder(s) participating in the RFP process need to fulfil the eligibility criteria given under this RFP document

### 3. Eligibility Criteria

J&K Bank shall scrutinize the Eligibility bid submitted by the bidder. A thorough examination of supporting documents to meet each eligibility criteria (Annexure D) shall be conducted to determine

the Eligible bidders. Bidders not complying with the eligibility criteria are liable to be rejected and shall not be considered for Technical Evaluation.

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

#### 4. Brief Scope of Work

The Solution will be based on OPEX Model where Successful Bidder shall will procure/Implement/Manage/Maintain a private cloud for Bank. Bidder will be responsible for handling all aspects of Network/Infra/Services/Applications/Switch and any other dependency of cloud. Bank Should be given necessary access of established cloud for conducting periodic performance and compliance assessments to assess system, processes and controls but all its management i.e, end to end management will be sole responsibility of Bidder. Bidder will deploy all network related links/devices/components required to communicate with Bank's Datacentre and DR for integration with Bank's applications like CBS, Mobile Banking, Aadhaar vault etc.

**UPI/IMPS Switch Integration:** Bidder should integrate their UPI Switch with Bank's existing systems (CBS delivery channels like ATM, POS, ECOM, and Mobile Banking) seamlessly, ensuring compatibility and facilitating the effortless operation of UPI acquiring services.

**Merchant On boarding:** Bidder will provide dedicated team to support the On-boarding of merchants, providing the necessary tools, training, and support required for swift and secure initiation of UPI payments. Bidder will be the face for Merchants and sub-members (DCCBs, PACS). Bidder has to handle all the support and escalations.

**Consumer Onboarding:** Bidder should provide dedicated team to support consumer Onboarding, Bidder should provide the necessary SDKs, tools and necessary support.

**Transaction Processing:** Bidder UPI Switch should handle the processing of UPI transactions, ensuring fast and reliable authentication, authorization, settlement, and reconciliation of payments.

**Risk Management and Fraud Prevention:** Bidder should apply advanced risk management techniques and fraud prevention measures to protect the Bank and merchants from potential threats, thereby ensuring secure and reliable UPI acquiring services. Bidder has to integrate UPI/IMPS Switch with the Banks EFRM solution.

**Analytics and Reporting:** UPI Switch should provide comprehensive analytics and reporting capabilities, empowering the Bank and merchants to derive valuable insights from transaction patterns, customer behaviour, and performance metrics to enhance their business strategies.

**Technical Support and Maintenance:** Bidder should provide round-the-clock technical support and maintenance services. Bidder should promptly address any issues, ensuring uninterrupted UPI acquiring operations for Bank and merchants.

**Bidder should have UPI Issuer solution with below features:**

- Single click 2 FA authentication aligned with regulatory guidelines
- Registration for UPI
- Payment address creation
- Setting UPI PIN
- Addition of account to VPA
- Removal of account from VPA
- Push transaction
- Pull transaction
- Mandate registration/ de-registration (for utilities, school fees, subscriptions, IPO mandates etc.) with a one-time secure authentication and rule-based access
- De activation of UPI account
- Balance enquiry
- Merchant registration
- Transaction listing
- QR code generation: Static and dynamic QR code issue to MSCB customers and sub-member bank customers including individual and institution
- Static/Dynamic/International QR Scan
- Provide QR code, Merchant mobile app
- Static/Dynamic/International QR Scan and pay
- Voice Out
- Peer to Peer P2P & Merchant Payments P2M
- Collect Request (UPI ID)
- Virtual address management (PSP virtual address, Merchant specific virtual address etc.)
- Ability to use Global address management like Aadhaar number, mobile number, in a unified way.
- Merchant Payment with single application or In-App payments
- Utility Bill Payments
- Collection, Donation, Disbursement
- Connect with service providers (Travel, Ticket, Utility bill payment, prepaid recharge (Mobile, DTH)) and aggregators
- Reports for Reconciliation
- Bulk Payment/ Bulk Collect
- Ability to raise complaint from Mobile App
- Online Dispute Resolution (UDIR) as per RBI and NPCI guideline MIS reports, uptime reports, Misc reports, transaction history, transaction logs, audit trails
- Reconciliation and settlement as per NPCI guidelines

- Solution should directly interface with NPCI, CBS, Mobile Banking, USSD, IVR, Internet Banking etc.
- The proposed solution to have interface with Bank's CBS

#### UPI acquiring features

- Merchant registration
- Merchant VPA creation
- Transaction listing
- Static and dynamic QR code issue to customers and sub-member bank customers including
  - Individual and institution.
- Collect Request (UPI ID)
- Standing Instruction / Auto Pay
- Reports for Reconciliation
- Merchant Payment with single application or In-App payments
- Merchant Settlement
- UPI Transaction & status check API for merchant integration
- Merchant Portal
- Dispute Resolution as per RBI and NPCI guideline
- Charges Module
- Reports - Standard Daily / Monthly Reports & Customized reports

The bidder has to comply with the Technical Specification and Functional Specification at **Annexure E1 and Annexure E2 respectively**. The bidder has also to comply with the Compliance Requirements and Hosting Assessment Checklist of the Bank, provided under **Annexure-M and Annexure N respectively**.

### 5. Broad Scope of Work

The scope of work should be read along with the technical specifications to ensure complete compliance to the scope of work. The solution proposed should be integrated seamlessly with the existing alternative channels along with NPCI solution. The bidder is also required to migrate the data from existing solution to new platform. Scope of supply includes Applications, Software components required to render the system offered complete in all respects even though every individual items may not have been specifically mentioned in the RFP. Bank will award the contract to the successful bidder who shall deliver the solution with the detailed scope mentioned in the Technical Requirement in Scope of Work. Also the solution must be cloud agnostic where bank may ask successful bidder to migrate the entire solution to Bank's Private Cloud or on-premise setup in future. Bank will bear the migration cost at that time after negotiations.



Bank will award the contract to the successful bidder and the bidder should deliver the service and the scope shall be but not limited to the following:

### 5.1 General Requirements:

1. Bank needs a robust enterprise-wide solution for Unified Payment Interface (UPI) to facilitate Interbank Funds Transfer for inward and outward transactions and solution should comply with “Master Direction on Digital Payment Security Controls” and other directives by Government/NPCI/RBI/NCIIPC.
2. Bidder shall provide Mobile Applications (Apps) for Android and iOS. The Bidder will provide the Mobile App for any other platform as desired by the Bank. The Mobile Applications should be based on latest technologies with high emphasis on security. The UI/UX interface should be intuitive & eye-catching.
3. The solution should be implemented on successful bidder’s hosting environment on Test/Dev/DC & DR setup. The entire setup will be managed and maintained and end to end implementation shall be be responsibility of Bidder. Bidder must implement extra Reporting Database setup that will be in Sync with Production Database and access must be provided to bank team for any reporting or any other purpose.
4. The solution should be adhering to NPCI UPI/IMPS technical specifications and Procedural guidelines for all the UPI/IMPS products (including various Operating Circulars (OC)) from NPCI.
5. Solution should be capable of adopting any future regulatory/ statutory requirement and any new additional functionality by NPCI without any additional cost to the Bank and timeline as specified by the NPCI / Bank.
6. Unified Payment Interface (UPI) & IMPS solution proposed should be capable of working under cluster with high availability (HA) at application and network, both at DC & DRC.
7. Unified Payment Interface (UPI) & IMPS should be capable of processing peak upto 1500 Business TPS with at least 500 TPS at the time of go live.
8. Unified Payment Interface (UPI) & IMPS solution should also facilitate online DC- DR (Cloud to Cloud) data replication and retrieval capability in a seamless manner. Bidder has to supply and install the required software at near site to DC to ensure zero data loss.

9. The proposed solution should be integrated with the Bank's Alternate delivery channels i.e. ATM, Internet Banking, Mobile Banking, SMS Gateway, Bank's CBS, Enterprise Service Bus /Payment Hub, SDR (Bank's Data warehouse), USSD, Financial Inclusion gateway, Multi- Function Kiosks, Remittance agencies, Third party PSP, WhatsApp Banking, Payment Gateway, E-Mail, Call Centre, CRM, CMS , Omni Channel etc. without any extra cost to Bank.
10. The bidder shall provide SDK (software development Kit) of UPI services for embedding the same in Bank's Mobile Banking application or any other Digital Banking Applications as per the requirement of Bank without any extra cost to Bank.
11. Bidder is required to provide SDK of the UPI features as per Bank's Brand Guidelines i.e. Design Library System for Android and iOS for incorporating in Banks's Applications without any additional cost to the Bank.
12. All updates and customizations shall be imparted in SDK simultaneously.
13. Bidder is required to provide multiple entry points for most commonly used features like Scan and Pay to Contacts, Pay to UPI ID, UPI Lite, Add Money, Collect Money etc. as required by Bank without any additional cost to the Bank.
14. The UI/UX for the UPI app and SDK to be as per the design approved by the Bank and need to be changed / updated as desired by Bank from time to time.
15. Solution should be capable of processing Bulk transactions through file upload for UPI Payment address creation, Push Transactions, Pull transactions etc.
16. The solution should be PCI-DSS compliant.
17. The Solution should run on OEM supported Container platform.
18. Solution should have APIs for all UPI operations/ transactions which includes issuer and acquirer functionalities like (this is an indicative list, any new functionality which is added during the contract period to be provided in the app) Functionality such as:
  - Registration for UPI
  - Payment address creation
  - Setting UPI PIN,
  - Addition of account to VPA,
  - Removal of account from VPA,
  - Push transaction,
  - Pull transaction,
  - Mandate registration/ de-registration including IPO mandates,

- De-activation of UPI account,
- Balance enquiry,
- Merchant registration,
- Transaction listing/History,
- Fund Transfer through Account+IFSC
- Static/Dynamic/International QR Scan (Online + Offline),
- Voice Out on Merchant application provided by bidder.
- Peer to Peer P2P & Merchant Payments P2M,
- Collect Request (UPI ID),
- Reports for Reconciliation,
- Bulk Payment/ Bulk Collect
- Integration with Payment Aggregators like BBPS etc.

19. UPI features / products

- Standing Instruction / Auto Pay,
- UPI Global transaction,
- E-Rupi,
- UPI-Lite,
- ICCW (issuer & acquirer),
- ICD (Issuer & acquirer),
- Delegate Payment/ UPI Circle
- UPI Central Mapper,
- Credit Card on UPI,
- UPI123,
- UPI UDIR
- FIR & FOR (Foreign Inward Remittance & Foreign Outward Remittance),
- UPI International
- UPI Now Pay Later (Credit lines on UPI)
- Voice enabled UPI Payment
- UPI Tap and Pay
- Any other UPI Features & functionalities launched by NPCI till contract period with no additional cost to bank.

20. The proposed solution should have interface with Bank's CBS through ISO (Connect24) or APIs or through Enterprise Service Bus/Payment Hub / Middleware as desired by Bank.

21. The proposed solution to implement the following products as per NPCI specification

- PSP platform
- Customer on-boarding

- Merchant on-boarding
  - Payment transactions (Push & Pull)
  - Communicate with UPI host
  - Receive inward transaction and respond
  - SMS integration
  - E-Mail integration
  - Integration with other service providers (Travel, ticketing, utility bill payment etc.)
  - Integration with BBPS vendor (for pre-paid and post-paid) and provide journeys
  - Interface with mobile app server.
  - Virtual address management (PSP virtual address, Merchant specific virtual address etc.)
  - Global address management like Aadhaar, mobile number
  - Single click Two factor authentication
  - Charges module
  - API support for all channels such as Mobile, Internet Banking, ATM etc.
  - Reports - Standard Daily / Monthly Reports & Customised reports
  - Support four party architecture as defined by NPCI
  - Transaction history
  - Hot listing of registered users account through self-service means
  - Encryption support
  - Any other functionality, UPI Features, Integration with other channel etc.
22. The bidder shall upload and publish the PSP app(s) in Android Playstore/iOS App Store.
23. Bidder must provide L2 Resources Onsite as desired by the Bank for Support/Product Management & Implementation of all Bank's requirements and Regulatory compliances including OCs.
24. The solution should be able to integrate with the Bank's UPI infrastructure (existing UPI switch), Internet banking, FI and credit/debit cards to enable merchants to link their UPI IDs and perform transactions seamlessly.
25. The platform / solution should be capable of connecting with database where customer KYC will be stored, to verification and Ckyc process.
26. The platform should integrate with KYC HUB for preform customer KYC.
27. The platform / solution should be capable of PAN verification (from NSDL), Aadhar verification (from UIDAI), Udyam verification (Ministry of MSME) and GST (GST Council) for any merchant on-boarded or to be on- boarded

28. The sensitive information/ Personally Identifiable Information (PII) when displayed on the screen should be masked, and be visible only to intended user.
29. The sensitive information/ Personally Identifiable Information (PII) when displayed on the screen should be masked, and be visible only to intended user.
30. The solution/software developed should follow a standard software development lifecycle process to ensure that it meets functional, security, performance & regulatory requirements of the Bank.
31. The issuance of UPI ID or pre-printed/regular QR codes should incorporate robust security measures to prevent fraud and unauthorized access. Data encryption and security measures with monitoring systems to safeguard the UPI ID or QR codes and the associated transactions.
32. The platform / solution developed should be scalable and adaptable to accommodate the growing needs of the bank and its merchant network. The system should be able to handle increased transaction volumes and support future enhancements or updates.
33. The aspect of data confidentiality shall specifically be taken care of while designing the solution.
34. The Bidder should host the solution in High Availability mode, along with DR and a minimum uptime time of 99.95%. The bidder shall do proactive monitoring and capacity planning at regular intervals and upgrade the solution. However, there should not be any additional cost to the Bank for any software upgrade during the contract period.
35. The Bidder has to maintain and manage the OS and Database every time the licenses are purchased by the Bank if migrated to OnPrem.
36. The bidder to design & size the hardware required at DC (Including Test / Development / Training) & DR. The Bidder should provide complete information on hardware requirement for end-to-end solution. Bank will provide required Hardware and Database for the proposed solution based on the sizing if migrated to On Prem setup.
37. Bidder should also provide security set-up proposed in the solution and various layers of risk identification and mitigation measures
38. The Bidder should provide the complete documentation including technical, operations, user manual, project plan etc.

39. Integrations with multiple internal and external systems through APIs. All these APIs should use hardening, tokenization and encryption. It should not use hard coded authentication. APIs should be routed through API gateways.
40. The Bidder should perform integration testing followed by user acceptance testing. The UAT includes Functional tests, Resilience tests, Benchmark Comparisons, Operational tests, Load tests.
41. Proposed software solution must comply with the IT Security Policy, Cyber Security Policy and IT Policy of the Bank.
42. Accepting payments through Bank's payment gateway, the integration should follow two factor authentication, captcha for login, and OTP confirmation on registered mobile for payments.
43. The solution shall be integrated with antivirus / anti-malware solution for scanning of files/ documents uploaded by the Customer's in support of their complaints / grievances.
44. The bidder shall adhere to Bank's Information System Security Policy (ISSP) , Supplier Security policy etc
45. The Bidder should be able to implement two-factor authentication wherever required in the solution / platform.
46. The Bidder shall be responsible for installation and management of any open source applications / technologies in the solution. Furthermore, the bidder should support, manage, maintain, and update any open source applications / technologies used in the development / deployment of the proposed solution.
47. The Bidder should integrate the application log trail with CSOC/SIEM, PIM, PAM for analysis related to cyber threats.
48. Integration with Multiple Banking systems which include more than one sound box solutions, Mobile Bankings, Ebanking, Kiosk banking, ATM Switch etc.
49. All Portals provided must have Bulk upload/Download options for transactions and Bulk deregister, Bulk block of UPI based on VPA/Account/Phone number, Bulk sound box

linking and delinking, Bulk unblock or customers etc. Bank can provide any specification for any change or implementation and Bidder has to abide by it.

#### **5.1b Cloud Agnostic Deployment Model and Migration:**

- a. The solution should be deployed in a lift and shift model and should be cloud and infra agnostic. The deployment model should have the capability to be migrated and deployed to any other Cloud /On-Premise Infrastructure in a lift and shift manner.
- b. Bidder will have to migrate the solution to Bank's Private Cloud or on-premise setup at any given time as decided by the Bank .

#### **5.2 IMPS Platform /Solution**

IMPS application to support the following functionalities

- IMPS 2.0 / IMPS 2.5
- XML based transactions
- All regulatory compliances / circulars / OC's to be delivered within regulator defined timelines during contract period.
- IMPS using Mobile number P2P (2.0,2.1)
- IMPS Using Account number & IFS Code (P2A)
- IMPS through Mobile Banking/Internet banking/Kiosk/Branch/Bulk/ATM
- IMPS through Branches (Portal available at Bank's branches for performing IMPS transactions)
- UDIR - Unified Dispute and Issue Resolution / ODR for IMPS
- For IMPS, Bank would prefer to expose only 1 channel / link towards the Bidders Infrastructure. Bidder will have to place an architectural pattern whereby a centralized software component performs integrations between applications. All channels ie. CBS, Mobile banking, internet banking, kiosk/FI, ATM would connect to this component and this component will further connect to the bidder hosted infra.
- All OCs and regulatory guidelines issued must be implemented without any additional cost to bank.
- IMPS Bulk handling and IMPS through Branch Channel with Application or portal to be provided to branch for transaction initiating.
- Transaction Portal must have users distinguished based on branch ID.
- Maker checker mechanism and two factor Authentication for all portals.
- All APIs and integrations to be provided by Bidder with all Bank's applications like Mobile Banking, E-banking ,Kiosk,FI,Debit switch , credit Switch etc.

### 5.3 Merchant Acquiring Platform:

The proposed solution and services shall assist the Bank in onboarding and managing both new and existing merchants in order to foster customer connections and therefore grow the Bank's UPI (Unified Payment Interface) business. Bank has below major requirements:

#### A. General Requirements

1. The bidder's solution should be capable of managing online as well as offline merchant



requirement.

2. Bidder should have experience of end-to-end merchant management lifecycle including Technology, Operations and Customer Support.
  - Technology
  - Operations
  - Customer Support
  - Offline Payments including software, device and complaint management
  - Online Payments - API and SDK driven platform
3. The solution should be capable of complete merchant lifecycle in UPI ecosystem for ETB and NTB.
4. The bidder should provide Merchant solution over QR code, API and SDK.
5. The bidder should provide services for On-boarding of merchants and obtaining KYC details through Tabs/Mobile App/Web App.
6. The Bidder should be capable to generate Pre-printed and regular QR codes that adhere to the UPI/NPCI guidelines as per the Bank's requirement. Bidder should be able to on-board online merchants as per UPI/NPCI guidelines.
7. Bidder should integrate the platform with Bank's UPI ecosystem through Bank API Gateway for sound box/device, portal, Merchant Mobile App online API and SDK.
8. Bidder should provide solution for Sound box or Voice out on Merchant Application with:
  - Pre-installed SDK for Merchant solution
  - Multiple language
  - Device specific SIM configuration
9. Purchase order would be placed by the Bank as per the requirement from time to time.
10. There should be proper system for the storage, distribution, linking and de-linking and destruction/purge of the UPI ID or QR code and related data.
11. Bidder should be responsible for the customer/device data security and should follow all the compliances required under payment guidelines.
12. The Bidder's solution should support smooth on boarding of merchants and customers onto the UPI ecosystem. This process should be user friendly, fast and require minimal documentation.
13. Bidder should be able to provide single point of reconciliation for all payments to merchants.
14. The Bidder should provide a solution comprising of both a web based as well as a mobile application for zonal offices/Head Office and branch officials, business correspondent agents at the field, respectively.
15. Bidder should be able to provide a dashboard to merchants to Monitor key metrics and view analytics important for business growth. Such as:
  - Complete Merchant details
  - Sub-ID details

- Real time Transaction Report
  - Reconciled Settlement
16. The solution shall support for migration of existing merchants which are already on boarded by the Bank.
  17. The bidder should provide required business, operation and technical support on the solution provided
  18. The bidder should provide support in person or through telephone and E-mail on
    - Claims/complaints
    - Mobile App
    - Web Portal
    - Integration support
    - Training videos and Demo
  19. The Bidder should carry out the implementation on premises by deploying required resources at Bank HO location / premises.
  20. The detailed functional and technical requirements for the implementation, customization and maintenance of Acquiring and providing UPI Merchant Digital Payment Solution are as under:

#### **B. Functional Requirements**

1. The bidder should generate the unique identification number.
2. The bidder should create a platform for issuance of UPI ID or QR Codes to verified merchants.
3. The Solution should have capability of on boarding ETB and NTB customers as Merchants. Proper verification and due diligence.
4. On-boarding of merchants should be done (existing or new) by providing solution to collect all the relevant documents such as signed Application form, ID proofs, address proofs, merchant agreement, etc. and by providing solution to upload softcopy/photo of the same.
5. The solution should be capable of doing real time verification of KYC, PAN, Aadhaar, Business Proofs, etc., before on boarding the customer.
6. The KYC verification shall be done using V-KYC service of the Bank. The proposed platform shall be integrated with Bank's VKYC platform.
7. The solution should be capable of activation of merchants (existing or new) and issuance of UPI ID or QR code to merchant with successful penny drop transaction.
8. The Solution should have the choice of all variety of merchant categories and codes.
9. The solution should provide the capability of managing the implementation of UPI ID or QR Code along with sound box, preprinted KIT, SOP for self on-boarding, instructions, welcome letter and user manual for settlement, reconciliation & report generation.

10. The solution shall be capable to integrate with UPI switch for Payment Voice notification (in Hindi, English and Regional Languages). Also capable to customize the voice delivery.
11. The bidder should provide merchant on boarding platform for Merchant/customer self-registration.
12. The solution should provide auto generated downloadable Merchant Agreement Form
13. Logins to portal and app, should have access control, two factor authentication, need based access, role based view, encryption etc.
14. The Solution should have capability of easy reconciliation process.
15. The solution should support Virtual Account for instant collection.
16. The Modules of the platform / solution for onboarding and issuance of UPI ID or QR should provide login rights / access as mentioned below:
  - a. Web application for Admin Dashboard for ZO, HO and Branches
  - b. Mobile application and Web application for Bank field officer, Merchant, Business Channel Partner (BC)/ Agent/Apprentice, etc.
17. The Admin login Branch/ ZO/HO module should have the following functionalities:
  - a. Merchant Management and Role permission
  - b. Branch Management and Role permission
  - c. Add/Remove/Modify Bank users/Business Channel Partner (BC)/ Agent / Apprentice by entering details of Aadhaar, PAN, business proof and photo of the individual)
  - d. Device management
  - e. Reconciliation Data
  - f. Allot QR codes to ZO/Branch
  - g. Real time QR issuance statistics and analytics
  - h. Download required reports
  - i. Capable of targeting specific group of Merchants by sending specific messages/emails.
18. Web Portal / Mobile application for Bank staffs / Agents / Merchants / Apprentice / CSP:  
The web-based portal should not require any kind of software installation and should be accessed from a device wherever there is internet access. The Mobile application should be available in both Android and IOS versions. Few of the features of the application/portal are listed below:

**C. Merchant application features:**

1. Login module should allowed user to register through application using OTP.
2. Dashboard with Real-time Transaction analytics and summary of daily sales/expenses

3. Sub merchant management with Maker and Checker configuration.
4. Complaint Management
5. QR generation (single/bulk) Static as well as dynamic QR
6. View/ download QR
7. QR code sharing option / Link sharing for payment
8. Transaction dashboard
9. Real time transaction monitoring
10. Real time settlement options
11. Sub merchant Management
12. View and manage settlements
13. Statement (View/download/ E-mail)
14. Sound box integration Request
15. Manage transaction details of customers & vendors
16. Send payment link & payment reminders
17. Channel Based Payment - SMS, E-mail and WhatsApp
18. In-app voice notifications
19. GST Invoicing
20. Generate Invoices in Bulk for Multiple Customers
21. Set expiry date and late fine for payments
22. UPI e Mandate- Recurring Payments
23. Availability of Festival Greetings and Customized Greetings.
24. Agent based collection with real time payment notification to admin & sales officers.
25. Offers and Promotions : Run Birthdays / Anniversary Offers, Create & Share Discount Coupons.
26. Subscription Plan and Payments: Create & manage different subscription plans, set

subscription expiry date, share plans/ renewal notification, Payment reminder, Auto Pay facility.

27. Integration with WhatsApp/SMS/e-mail for receiving payments receipts.

28. Mobile / Tab application should be fully secured with the following:

- Device Binding shall be done for the merchant application for more security
- Two-factor authentication
- End-to-end encryption
- Encrypted data transmission across channels

19. The Solution shall be capable of handling the different types of merchants with different hierarchies.

20. The application should provide users with the ability to customize their experience, such as choosing their preferred language and setting up personalized alerts.

#### **D. Facility for Merchant:**

1. Separate application for merchant which enables merchants to do all activity such as single/bulk Pay/Collect transactions using various options like VPA/Biometric/QR code (Dynamic, Static, Bharat QR code), generate customized reports, transaction enquiry etc.
2. Merchant Management
  - Merchant On-boarding (Single as well multiple terminals)
  - Adding Merchant Association
  - MIS Reporting for a particular Merchant
3. Customized API/SDK and other integration support to provide following facility to merchant:
  - Web Collect / Web QR facility
  - App intent facility
  - Integration for generation of Dynamic QR for collecting payment
  - Payment of Bill through the Dynamic QR printed in the Bill (either Physical or sent through email)
  - Bulk Collect Request processing and monitoring
  - Generation of Dynamic QR through handheld device
  - Static QR generation for shops /offices with agent option and well-defined hierarchy
  - Dynamic QR/VPA collect facility for Cash On Delivery (COD) option
  - Centralize Collect facility
  - UPI solution for POS/ MPOS
  - Integration with the chat platform where SDKs (Software Developer Kits) and APIs are provided by the Bank and UI is designed by the chat platform.
4. All possible solutions for all type of Merchants such as Web Base (API), Mobile Base (SDK), offline mode (QR Code and others) for merchants who are using separate accounting application like Shopping Mall, Offline collections etc.

5. Integrate UPI with Payment Aggregators as requested by Bank

**E. Bank Staffs / Agents / Apprentice / CSP application features:**

1. Login module should allow user to register using OTP
2. The KYC verification
3. On-boarding of merchants (existing or new)
4. Activation of merchants (existing or new) and issuance of UPI ID or QR code to merchant with a successful penny drop transaction
5. Complaint management module
6. View and manage settlements
7. Supports integration Third party Services - (Account Purpose)
8. UPI ID or Dynamic QR code generation
9. Inventory management with status delivered, destroyed, issued, etc.
10. Reports:
  - a) All statutory and regulatory reports as required by the regulatory institutions.
  - b) The Bidder shall have to provide all the MIS reports as per the requirements of the Bank.
  - c) The platform / solution should have the capability to collect and analyze data generated from the platform
  - d) / solution and from other applications of the bank, to generate real time / near real time analytics.
  - e) The Bidder shall have to provide the Bank weekly progress reports on the bugs/problems reported/points taken up with schedule of date of reporting, date of resolving, and status for all kind of bugs and problems whether reported by bank or Bidder.
  - f) The application should use data visualization techniques, such as charts and graphs, to present the information in a clear and easy-to-understand format.
  - g) Reports shall be kept as archived and vendor shall arrange to provide any adhoc reports for any period (minimum of 3 years) during the contract period to Bank.

#### **5.4 Infrastructure:**

The bidder shall , customize, implement and maintain UPI and IMPS Switch and other related services along with all necessary software, middleware interface, APIs, UPI Applications (Android & iOS), SDKs, Merchant Solution including Portals etc. as mentioned in the RFP. The bidder shall also procure, maintain and manage underlying hosting infrastructure.

The Bidder needs to size the infrastructure (Servers, network switches, HSM, Operating System, APM, containerization platform and other related hardware/software etc.) for the solution based on the volume and the growth indicated in the Growth Volume Projections

### 5.5 Current Transaction Volumes and Growth Projections:

Current Volumes in UPI and Projection for number of transactions in the Mentioned Month

| Year on Year | UPI/IMPS Transactions<br>(Financial Plus Non-financial)<br>Monthly | UPI/IMPS Transactions (Financial<br>Plus Non-financial) Yearly |
|--------------|--|--|
| April 2025   | 26 Crores  | Financial Year 2025/26 (312 Crore)                             |
| April 2026   | 36 Crores  | Financial Year 2026/27 (432 Crore)                             |
| April 2027   | 55 Crores  | Financial Year 2027/28 (660 Crore)                             |

The transactions count is based on Assumption of 40% YOY growth as per current truncation value. Actual number may vary from the projected value and may be more than 40%. The Bidder has to ensure that the platform should be scalable to handle such load in future.

Following is the minimum required list of infrastructure components to be provided by Bidder and same need to be factored in the technical / commercial bid. Apart from the components listed below, Bidder has to provide any additional Software components required for the successful implementation of the project.

1. Software for application, web, middleware server etc.
2. Reporting tool
3. Any other software item required for UPI/IMPS Switch functioning

The end-to-end implementation, maintenance and support of the Unified Payment Interface (UPI) & IMPS solution on OPEX Model shall be part of the scope of the bidder.

As part of the technical proposal the bidder needs to provide complete Unified Payment Interface (UPI) and IMPS solution details. The bidder must design the solution with high availability, Active-Active setup & secure Infrastructure in Data Centre and Disaster Recovery site ( Hosted Model ) as per Industry accepted security standards and best practices.

The Application & Database should be sized for Active- Active cluster at DC & Active- Active cluster at DRC, so that the solution and infrastructure can fall back on each other. The Proposed solution should be containerized and based on micro-services architecture, so that new services deployment will have zero down time. DC - DR replication should be available as part of the solution so that in case of switch over the complete solution should seamlessly work. Bidder has to also establish near disaster recovery site for achieving zero data loss in case of disaster.

The bidder shall install and maintain the software as required by the solution. Bidder shall also maintain the hosting Infra and all necessary configuration, parameterization etc. Bidder has to resolve the issues arising during integration of other component (like webserver) or software (like Database, Enterprise Service Bus /Payment Hub & other third-party software). The performance tuning & parameterization of Database & other software to support smooth running of the application, should be done by Bidder.

Bidder needs to accordingly provide as part of the technical solution the complete UPI Switch details like Application, Software and other related software requirements. The details shall include:

1. List of Applications, Software along with licensing details (Including installations and replication at DC and DR).
2. Details of redundancy and security setup.
3. Application architecture along with a detailed diagram including the infrastructure setup.
4. Implementation procedure / road map.

The Bidder is responsible to arrive at the sizing independently based on the volume and the growth indicated in the Growth Volume Projections table.

The Bank will not be responsible for any assumption made by the Bidder with respect to the sizing. In the event the sizing proposed by the Bidder does not meet the performance / service levels of the Bank, the Bidder will carry out the necessary upgrades / replacements.

The bidder shall ensure that the solution is complied with all the regulatory guidelines of GOI/ RBI/NCIIPC/NPCI and also adheres to requirements of IT Act (including amendments in IT Act and its Rules thereof). A self-declaration to this effect shall be submitted by the bidder.

The submitted Hardware Sizing for UPI/IMPS Application and other Softwares by the Bidder should not be over-utilized. The utilization of Hardware should not be more than 70% during the whole contract period. The Bidders should Size the Hardware accordingly.

CI/CD pipeline will be designed, implemented and managed by the UPI Application Service bidder.

Bidder has to design and install the UPI Infrastructure to meet the Bank's requirements and provide the Certificate that the proposed Infrastructure will successfully handle the projected volumes & peak business TPS.

### **Benchmarking:**

The proposed solution should be benchmarked for 1500 peak Business TPS (Transactions per Second) and able to handle 40 million transactions per day on go live day. Bidder has to demonstrate the volume handling capacity of the UPI system and provide load and stress test reports of same.



The bidders should size their UPI Application and other Software envisaging the 40% growth in peak TPS per year.

Bank can deploy any number of instances of UPI/IMPS Application & can segregate the UPI/IMPS switches based on Issuer/Acquirer/PSP or any such combination. UPI Switch Application based on Opex model can be used at unlimited Hardware without no additional cost to the Bank.

The Bidder needs to size the infrastructure (hardware, Operating System and other related Hardware/Software) for the solution based on the volume and the growth indicated above and propose the same as part of their technical bid submission. The Applications & other Software provided by the Bidder should work in any number of Hardware/Devices without any extra cost to the Bank. However, the complete implementation, maintenance and support of the Unified Payment Interface (UPI) and IMPS solution shall be part of the scope of the bidder. The performance tuning & parameterization of Database & other software to support smooth running of the application, should be provided by Bidder.

Bidder needs to accordingly provide as part of the technical solution the complete IT infrastructure details like Server, Operating System, Storage Capacity and other related requirements.

The details should include: -

1. List of Hardware, Operating Systems (OS), Databases containerization platform etc. on which the solution is compatible along with licensing details for the complete solution (Including installations and replication at DC and DR).
2. Details of redundancy and security setup.
3. Application architecture along with a detailed diagram including the infrastructure setup.
4. Implementation procedure / road map.
5. Proposed Server and related infrastructure specification required as part of the solution implementation (for DEV/UAT, pre-production and production setup) along with the quantity to meet the Bank's redundancy requirement.

The Bidder is responsible to arrive at the sizing independently based on the volume and the peak business TPS growth indicated in the RFP.

## 5.6 Migration of Data from existing UPI Switch:

1. The bidder shall establish an interface between old switch and the new switch

2. The bidder should migrate all customer and transaction data from current switch to the new switch while maintaining confidentiality and integrity of the data.
3. Complete Data Migration from old UPI switch to new/ proposed UPI switch without any data loss.
4. The bidder shall be responsible for migration of the switch data, from the existing switch to the proposed switch. All current functionalities and customizations available currently on Bank's Switch including on front end devices like UPI APP shall be migrated seamlessly by the bidder onto the proposed switch. The bidder shall also be responsible for migration of legacy data of existing system as part of the migration activity. It would be the responsibility of the bidder to coordinate with Bank's existing outsourced Switch service provider for migration of UPI switch data, from existing system to the proposed UPI switch with Zero loss and no change in the existing data taxonomy for all transaction processes. Similarly, end user interfaces functionality shall remain unchanged. The bidder shall ensure that migration is accomplished with all the existing conventions and concepts available in the legacy system.
5. Migration activities shall be divided into three main categories as described below:
  - Pre-migration Activities
  - Data Extraction and Loading of data in New Switch
  - Post-migration Activities

#### **A. Pre - Migration Activities**

Before migrating data from the Bank's existing switch; either automatically or manually; there are certain activities that need to be completed as pre-requisites related to cleaning up existing data. These activities shall be identified during the course of the data mapping discussions with the Bank's team.

#### **B. Data Clean up**

All the requirements of bringing the source data in desired, synchronized and integrated form shall be dealt by data cleaning up exercise undertaken by the bidder. Data migration activities shall ensure that the existing data inconsistencies would be brought to a common functional requirement. Missing or incorrect data shall be rectified before migration. However, this will be subject to appropriate decisions on the actions to be taken by the Bank. Taking into consideration the design and customization changes, unique keys for each table shall be identified.

Mock migration runs conducted by the bidder basis the data provided for migration, shall give indication about possible data clean up that needs to be taken up before actual data migration run.

### **C. Data Extraction and Loading in New switch**

Data required for automatic migration for each module shall be discussed by the bidder and separate documents for each of the modules shall be agreed and signed- off for that purpose in consultation with the Bank's team with existing vendor. This document would enlist the field-to-field details in the new switch, their mappings with the existing system fields, and corresponding action on each of them. The bidder shall carry out extraction of the data from the existing switch into new switch.

The bidder shall migrate the existing UPI switch network including replenishing the assets to their network. Towards this, the following steps shall be undertaken:

1. Test the new network before deployment with the Core Banking Solution / Enterprise Service Bus /Payment Hub, Middleware, carry out sample reconciliations and present to Bank for approval on tests and schedule.
2. Carry out migration of UPI Switch as well as data, as per schedule.
3. In case the UPI services are found to be non-functional at the customer or merchant end due to any reason during the migration, re-registration of such services shall be the responsibility of the bidder at no cost to the Bank.
4. Migration of disabled UPI accounts from existing switch to the new switch including archive data.

The bidder shall perform the Project Management/Program Management of all the activities related to the scope of services and conduct regular review with the Bank's team to complete the activities in a time bound manner.

### **D. Post-migration Activities**

The data that could not be converted due to reasons like unavailability in the extraction file or due to erroneous source values needs to be manually maintained as a post-migration activity. The data which is defaulted by the conversion programs due to non-availability in the old system might also be required to be enriched and modified later on for any corrections. The bidder and the Bank's team shall arrive at a consensus on manual migration of records based on the volume / number of records. The bidder shall have complete responsibility to migrate such records at no cost to the Bank.

The Bank would be conducting a post migration audit to verify the completeness and accuracy of the migrated data. The Bidder shall provide the Bank and the auditor with all required documentation evidencing the checks and balances applied by the bidder for the purpose of migration. The bidder shall remediate any observations arising out of this audit at no cost to the Bank.

## 5.7 Monitoring and Management

- i) Monitoring and Management of UPI solution including infrastructure shall be deployed. Bidder should provide the dashboard for Real-time monitoring of UPI transaction and facility to go up to the level of transaction (RRN) and getting the Transaction status and its reason of failure,

if any. Breakup of Business and Technical decline. The dashboard should also have the capability to generate reports like count of Financial & Non-Financial Transactions for a period, Number of Customers on-boarded etc.

- ii) Implementation & Migration of the Project will be performed Onsite i.e. at Bank premises only.
- iii) Configuration management. The successful bidder must ensure that all installed infrastructure & solutions are updated with the latest configuration and both the sites (DC, & DR) have consistent configuration.
- iv) Patch Management - The successful bidder must ensure that all installed infrastructure & solutions are updated with patches as and when they are released after due testing. Critical patches should be applied immediately as per Bank Policy.
- v) Service Level Management, Service reporting- The successful bidder must maintain the service levels as per the RFP and provide a periodic report to the Bank assessing performance under the scope of RFP against the Service Levels.
- vi) Change Management. The successful bidder must ensure that the required changes in the application & solution related changes are properly updated and recorded with version controlling and to have consistent setup all the sites (DC & DR).
- vii) Operation Management - The successful bidder should review the performance of the deployed solution / technology deployed on a Quarterly basis and make necessary upgrades, changes in the application setup & other hosting infrastructure as and when required without any additional cost to the Bank. The successful bidder should monitor measures, evaluates, and records status and performance information about all the equipment and software brought in by the bidder to aid in performance monitoring and tuning of the environment. Performance metrics should include utilization, throughput and other critical system needs. The successful bidder shall implement proactive procedures to address trends identified from performance and monitoring data. The successful bidder should provide standard reports that are to be provided to designated Bank personnel.
- viii) Successful bidder shall fix any security findings/vulnerabilities identified by various security agencies hired/consulted by the Bank without any additional cost during the contract period. Further, if the security observation(s) cannot be closed by applying updates/patches/fixes/upgrades to the setup and replacement is the only option to close the observation(s), then the successful bidder has to replace the softwares meeting all the specifications of the RFP at no extra cost to the Bank.
- ix) End of Sales / End of support: The bidder is expected to submit the bid for latest version of software/solution. The Bidder has to ensure that any solution and related components supplied as part of this RFP should not have reached end of support for at least 5 years from the date of issue of purchase order.
- x) Facility Management (FM). The bidder shall ensure that the FM personnel are available exclusively for UPI Switch Solution & Softwares. FM personnel shall have a graduate degree at a minimum, have 2 years of experience in the field of UPI Switch / relevant support and have in-depth knowledge of the solution provided. Bank reserves the right to interview the FM

personnel including Team Lead intended to be deployed and if not found suitable may reject them.

- xi) The bidder shall provide mission critical support for UPI Switch and other softwares. The mission critical support includes 24x7x365 support with site engineers for Application and softwares.
- xii) Incident Management :The bidder shall establish robust Incident Management process including:
- Provide 24 x 7 support for incident management for all Components of the UPI switch solution including Apps
  - Provide automated fault detection and resolution
  - Ensure system to do automatic dispatching to avoid delays and automated messages to Field / Support Engineers
  - Ensure system to provide for automatic escalation in case of problem not getting resolved.
  - Do proactive maintenance of all devices on cloud.
  - Analyse machine performance and suggest improvement.
- xiii) Service desk:
- Providing technical assistance for logging, troubleshooting and managing the service requests for the UPI application
  - Monitoring, alerting, troubleshooting and resolution of incidents/ problems for the UPI switch solution

## 5.8 Information protection

- Backup, storage and restoration of data related to the UPI switch and associated services, in a secure and reliable manner
- Backup, storage and restoration of configuration data for the UPI switch and associated infrastructure
- Backup, storage and restoration of any mission critical data related to the UPI switch and associated services
- Backup, storage and restoration to enable the Bank to achieve regulatory compliance and as per BANK ISMS & BCMS Policies, RBI, NCIIPC (National Critical Information Infrastructure Protection Centre), NPCI guidelines.

## 5.10 Business Continuity/ Disaster Recovery

- Implementing and maintaining BCP and the DR readiness (including data replication), for the UPI switch and associated services in order to meet the Bank's RTO and RPO Objective.
- Replication of data between the primary and the DR site from the disaster recovery perspective.



### 5.11 Compliance and assurance

- Assisting the Bank in attaining and ensuring on- going compliance to various regulatory and data security/ privacy requirements
- Addressing relevant threats/ risks identified in a proactive manner and through audit observations
- Providing analysis and MIS for Switch and associated services related data, to demonstrate audit readiness and adherence to the agreed service levels.
- For all existing applications, BIDDER shall submit Data Dictionary (wherever feasible) as a part of System documentations.
- submitting within 10 days from signing of this Agreement, an Application Integrity Statement from application system vendor providing reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs and free of any covert channels in the code
- Compliance to Bank IS policy and other related policy, adherence to Bank Minimum Baseline security requirement, adherence to Quarterly VAPT requirement
- Adherence to NPCI requirement for App certification/ re-certification / new functionality launching,
- Bidder should ensure that audit observations by Bank's Internal and External Auditors are closed in a time bound manner.
- Bidder will implement/adhere all guidelines/instructions of Government/ NCIIPC/ RBI/ NPCI etc without any extra cost to the Bank.
- Closing audit observations for compliance to various secure code review audit, App-sec audit, configuration audit, VA audit or any other Audit requirement raised by NPCI within the timeline given.
- Various Regulatory requirement such as Device Binding, SIM binding, unsecured Wi-Fi restriction, Encryption etc.

### 5.12 Disaster Recovery Mechanism

The proposed system must be capable of and compatible for Disaster Recovery Implementation with Recovery Point Objective (RPO) - 0 minutes and Recovery Time Objective (RTO) - 180 minutes. The successful bidder should describe the provisions for disaster recovery and show that the proposed solution facilitates disaster recovery. The

bidder needs to submit the technical architecture relating to data replication between primary and secondary site. Proper Backup policy should be considered in implementation plan.

The bidder needs to submit the technical architecture relating to data replication between primary and secondary site.

### 5.13 Detailed Solution requirements

1. The architecture of the UPI/IMPS solution should allow Bank's system to be easily integrated and the technology used should be easily adoptable and portable to the bank system.
2. Seamlessly migrate all the user registered for the Bank's existing UPI/IMPS app.
3. Integrate UPI with our systems such as CBS (B@ncs24), Enterprise Service Bus /Payment Hub / Middleware -IIB/CP4I, SDR (Bank's Data WareHouse), FI Server, Card Management System (CMS), Mobile Banking, ATM switch, Internet Payment Gateway, Net Banking, Aadhaar Pay, Aadhaar Data Vault, etc.
4. Integrate UPI/IMPS application with Banks Analytics solution, PIM solution, SIEM Solution, EFRM Solution or any other security solution as required by the BANK, etc.
5. Customer On-boarding App & portal, User Portal, Admin Portal, Customer Complaint module, UDIR, Marketing Module (Email, SMS etc.) and other interfaces required to handle UPI transactions.
6. Merchant On-boarding App & portal, User Portal, Admin Portal, Customer Complaint module, Marketing Module (Email, SMS etc.) and other interfaces required to handle UPI transactions.
7. Providing option for Bulk user creation from Back end and providing Option in Application to retrieve password through SMS/E-mail of such users.
8. VPA Management
  - Bulk VPA Creation - Ability to create Bulk VPA and associate Accounts
  - Customized and special VPA creation
9. Application should be enabled with send/receive notification through cloud Messaging platforms and SMS.
10. Notification through an alert (SMS/E-Mail) to system administrator/ technical team.

11. Security alert on registered mobile number on the account of excessive activity in the account (Bank expects an alert to be sent to customer, it can be either SMS or as an app notification (push)).
12. The system architecture should support any future integration with UPI, should also be feasible with or without major change. Necessary API and SDKs are required should be shared with the Bank.
13. The UPI/IMPS solution should have its own security features, so it does not process any request that comes from outside banking host system.
14. The solution should also include various audit trail reports for transactions made using Unified Payment Interface (UPI) and IMPS solution as and when requested by the Bank's internal/ external auditor. The vendor is required to conduct code review from any prestigious external agency and submit report. The vendor is required to fill the gap found in the audit report without any cost to Bank before going live.
15. The solution should be platform independent and scalable to support transactions envisaged by the Bank.
16. The proposed solution should:
  - Be designed with MACH (micro services, API, cloud native and headless), scalable, plug and play, composable, modular, independent and loosely coupled architecture
  - Adhere to below design principles for micro services architecture
  - Each micro service should have independent development, testing, integration, and support capability
  - Each micro service should have maximum reusability as well as separation of concerns
  - Each micro services should offer isolation of environment, configuration variables, data etc., and allow communication only through APIs
  - Replication of data across micro services should not happen
  - Each micro service should follow optimal design pattern per the business use case
  - Each micro service should generate logs in a centralized repository to be used for monitoring, and not store any log locally
  - Each micro service should integrate with centralized monitoring and performance telemetry tools
  - Each micro service should be cloud native by design

- Each micro service should allow deployment as-is on premise, private cloud, or public cloud without design changes
  - Micro services should support service discovery, service-mesh, and event streaming
  - The successful bidder should procure and provide any tools and licenses required to support service discovery, service mesh, streaming / messaging etc.
17. Bidder to provide log aggregation solution as part of the scope. Bank may at its discretion choose to integrate with alternate log aggregation solution available with bank:
- i) Leverage a container platform to build, host and run the microservices :
    - Underlying container platform should be compatible with on-premises, private cloud and public cloud installations
    - Single control plane should cover all possible deployments (on-premises, private cloud, public cloud etc.), while control plane should be deployed in on-premises or private network only
  - ii) Be architected to be fault tolerant and ensure cascading failures do not occur
  - iii) Be cloud-ready to support any future migration to cloud without requiring technical upgrades or customizations
  - iv) Support graceful exception handling, restart, self-healing or recovery process in the event of transaction or process failure
  - v) Support native, hybrid-web, and web apps
  - vi) Offer isolation to microservices layer from the public facing API gateway layer. Inter-service communication should not take traffic out of the layer in which the services are hosted
  - vii) Provide open APIs for integrations and conform to RESTful specifications
  - viii) Ensure API caching is implemented wherever data refresh frequency is low
  - ix) Provide APIs (with detailed documentation) for all omni-channel digital banking platform capabilities to integrate with other systems
  - x) API specs should be maintained using industry standards such as Swagger/RAML and should be versioned along with the API's code or configuration
  - xi) Support partner, fintech and ecosystem integrations through APIs, including catalog of digital services and APIs, automation features and accelerators for faster integration/on-boarding, and other best in class open banking features
  - xii) Provide CORS for whitelisted domains/origins
  - xiii) Ensure dynamic allocation of compute for load agnostic performance experience to customers
  - xiv) Implement horizontal scalability at module/service level to handle required transaction volumes and composable architecture
  - xv) Guarantee 99.95% availability for the proposed solution
  - xvi) Implement required integrations including core system integrations, partner, fintech and ecosystem integrations
  - xvii) Implement caching across all digital channels appropriately, including static data caching, images, web assets (CSS, HTML, ICO etc.)

- xviii) Implements mature in-memory caching capabilities with cache store located nearest to the source of the provider in compliance with data storage requirements
  - xix) Implement configurable caching strategy based on type of data sources, consumers, data validity etc.
  - xx) Implement capability to push notifications regarding new changes over the air without frequent uploading on app store of various platforms
  - xxi) Implement highly scalable communication methods such as asynchronous APIs, event streaming and message queues where appropriate (e.g. user event-based triggers, data streaming pipelines, click-streaming analytics, mission-critical applications etc.)
  - xxii) Implement standard optimization techniques (e.g. caching, parallel processing, support standard optimization techniques, etc.)
  - xxiii) Leverage automated testing and performance testing to improve quality and speed of delivery
18. The solution to have the capability to process transactions at the peak speed of 500 Business TPS on day of go live and should be scalable upto 1500 TPS as per the Bank's growth during the contract period.
19. Bidder should review the TPS data periodically (quarterly) and on ad-hoc basis in co-ordination with Hardware vendor or as and when required and maintain buffer of 30% TPS in addition to actual peak business TPS noticed during review frequency defined by the Bank. and bidder or as & when required by the bank.
20. Bidder shall provide a Web-Portal for fetching the RRN wise details for RBI/Cyber Security queries in the proposed solution.
21. Solution should integrate with different interfaces using standard message protocols like ISO 8583/ISO 20022, Web services, BizTalk, MQ server, XML based protocols, APIs etc.
22. The bidder should have sound knowledge of UPI transaction flow, ISO 8583/ISO 20022 and financial messaging structure and have the capability to implement the solution as per NPCI standards.
23. UPI solution should provide a drill-down Dashboard with current status of the system in display as below:
- a. Number of transactions processed from start to current
  - b. Transactions per second (TPS)
  - c. Real time transaction decline status including Technical Declines
  - d. Number of successful transactions
  - e. Number of status unknown transactions

- f. Number of failed transactions with response code
- g. Total running time in hours, minutes and seconds
- h. Status of original and Verification requests for a given transaction
- i. Business decline transactions for the day/month/year
- j. Technical decline transactions for the day/month/year
- k. Number of Reversals Processed (Debit & Credit)
- l. Number of Registrations done for the day/month/year
- m. Number of Transactions done by Other App and Bank's App
- n. Profiling of UPI Scenarios in production by configuring at User Level and/or Service Level

24. Additional features of the UPI solution

- a. Enable / Disable on screen log
- b. Enable / Disable file log
- c. Enable / Disable database log
- d. Reset on screen log
- e. Quick screen log - should show all transaction messages on screen, should have at least 100 transaction records on screen with limited data with no compromise to security. Option to clear the on-screen log should be available to wipe the data as and when required.
- f. File Log - All transactions have to be logged in to a flat file with a proper delimiter and in encrypted format.
- g. Database log - All transactions have to be logged in to database with all required data.
- h. **Alert and Notification:** Notification for System Exceptions -
  - Connectivity Down, Services Down, Application/Service down etc.
  - Configurable Notification for Business Violation and transaction failure
  - PUSH notification to customers for scheduled Downtime or as required by Bank

25. The log setting should be changed through the configuration manager using a front-end. All logs should always be available; no transaction should be performed without log. All logs' data should be encrypted and stored. Only through the front-end tool designed to view the log should be capable of displaying the data, no plain text should be stored in the log.

26. All administrative activities should be properly logged with proper audit trail.

27. The audit logs should be capable of being used for forensic Evidence.

28. Facility should set channel wise as well as transaction wise commission to be charged.

29. Facility should create different user groups with different set of rights/permissions.

30. The portal should support to work on maker and checker concept for any addition, deletion, modification request made by the authorized users.
31. Prepare a project plan and a resource deployment plan for implementing UPI solution in the Bank
32. Provide periodic updates on progress, risks, issues, and mitigation throughout the implementation phase.
33. Use Agile methodology and DevSecOps for the implementation to ensure evolving requirements are incorporated in a live platform.
34. Maintain code base of each microservice as a separate code repository, with best practices such as branches, tagging etc. Details of code ownership and IP are listed in the Licensing section.
35. Ensure all deployments across environments (development, SIT, UAT, pre-production, production) are directed through robust DevSecOps pipelines following stage-gated quality controls:
  - DevSecOps pipelines should cover all stages of development and operations including plan, code, build, test, release, deploy, operate and monitor
  - DevSecOps pipelines should have automation tools to enable continuous planning, continuous development, continuous integration, continuous deployment, continuous testing, continuous monitoring etc.
  - Stages for quality control should cover code quality, code coverage, static code analysis, unit testing, integration testing, functional testing, dynamic code analysis, and non-functional testing including performance tests, security scans etc.
  - Monitoring of quality gates should be enabled through a dashboard and a report should be shared with the Bank for all release cycles
  - Acceptance criteria for quality gates should be configurable and updated based on discussion with the Bank
36. Setup all tools and software required to enable above DevSecOps requirements including source code management, code review, code analysis, continuous build and deployment automation, release base management, automated testing, quality dashboard, backlog planning, log management, performance testing etc.
37. Ensure usage of canary and blue-green deployment strategy depending on the scope and take approval from the Bank to support zero-downtime during releases
  - Enable incremental feature testing with closed audiences



- Enable multivariate testing, ability to test efficacy by time, content, layout, customer segments etc.
- Push notification should be sent to users to notify about downtime (in advance and during the outage window), with estimated end time, contact details of support team or any other details required by the Bank.

37. Charges Management -Managing different types of charges/commissions (switching charges, merchant/retail usage charges, PSP app charges, Interchange Charges, cost Margin for MCC) required:

- PSP profile creation
- Registration for Bank Account (Own and Other Bank's Customers)
- De-registration from the UPI Application
- OTP Generation and Regeneration
- "Pay" (push) and "Collect" (pull) payments
- Two factor authentication using mobile and second factor (PIN/Password)
- Generation of Virtual address (Virtual address is an alternative payment address). The customers should have flexibility to define their virtual address.
- Payment using Mobile Number, Aadhaar Number, Virtual Address, Account Number IFSC code & MMID.
- Regular/recurring payment by one-time instruction and the revocation of the instruction, if required.
- Push / Notification Services
- Forget & Reset PIN
- Any other charge management module as asked by the Bank.

#### 5.14 Accounting and Reconciliation

- The proposed solution to provide a reconciliation related reports as required by the BANK / NPCI and make changes in the reconciliation reports as and when required / asked by the bank. The proposed solution to provide the report in real time cycle-wise in tune with NPCI Cycles.
- Recording and Storage of all transactions pertaining to the Switch and associated services, as described in the BANK and NPCI.
- MIS reports for all switching and associated activities on a routine basis, and as requested by the Bank.
- Ability to interface with the Bank's Reconciliation System to provide the reports required by the Bank, in the format as prescribed by the Bank

#### 5.15 Management Information System:

1. The solution should provide the complete reports/Dashboard/Customised Analytical Reports pertaining to UPI. This should include the risk management reports, various analysis reports in figures as well as graphical representation. All data should be real time, and data till current time should be available.
2. The MIS should provide following basic reports.



- Transaction summary
  - Transaction detail
  - Channel wise transactions (Payment Gateway, Net-banking, SMS, Mobile, Branches, ATM, USSD and Other mode of payments etc.)
  - Report pertaining to inward transactions
  - Report pertaining to outward transactions
  - Bank wise remitted transactions
  - Meta API transactions (non-financial)
  - Dashboard for Daily reconciliation, NPCI Report (NTSL)
3. Separate daily Dashboard report for performance monitoring and report for Installation and un-Installation of App.
  4. All these reports should work with for any date range given, the above are some of the basic reports, and the bidder should suggest and provide various other transaction monitoring reports.
  5. With respect to risk, following are the reports that are mandatory
    - One to many transactions
    - Many to one transactions
    - Suspicious transactions report based on different parameters set by the Bank/NPCI like velocity, geographical location, locality etc.
    - Remittance pattern of any given customer

### 5.16 User Acceptance Testing

- i) The bidder should assign a dedicated team for UAT with NPCI
- ii) UAT has to be done at bank specified premises incoordination with bank's designated teams.
- iv) Customization of the application software, if required has to be done by the bidder at no additional cost to the Bank based on the UAT observations and NPCI guidelines.
- v) Bidder should share the project plan and accordingly the team should work to complete the UAT on time. The project plan should include all important milestones and approaches to achieve the desired goals, e.g. Dry runs, Parallel runs, Roll-back plans, contingency plans etc. Illustrative Project stages are summarized as below.

| Stage                         | Deliverables  |
|-------------------------------|---|
| Project Preparation           | <ul style="list-style-type: none"> <li>•Project Kick-Off</li> <li>•Project Charter and Project Plan</li> <li>•Resource Deployment Plan</li> </ul>   |
| Business Design               | <ul style="list-style-type: none"> <li>•As-is report &amp; Identification of major / minor design consideration</li> <li>•To-Be report and Gap Assessment report</li> <li>•Workshop for business blueprint, gaps and way forward</li> </ul> |
| Configuration & Customization | <ul style="list-style-type: none"> <li>•Configuration document consisting of system setting and parameters customization-design, development and technical documents</li> </ul>   |

|                                 |   |
|---------------------------------|---|
| Integration                     | <ul style="list-style-type: none"> <li>•Integration with Bank's existing solution(s)/interfaces/NPCI etc.</li> </ul>  |
| UAT signoff in test environment | <ul style="list-style-type: none"> <li>•Demonstration of all the functionalities/ requirements as depicted in the scope of work along with all required customizations including interface with Bank's existing Infrastructure</li> <li>•Any necessary additional stress testing to be arranged by bidder</li> <li>•Resolving of UAT issues and signoff</li> </ul>  |
| Technical Documentation         | <ul style="list-style-type: none"> <li>•The document which needs to be delivered by the vendor to the Bank for every software/module including any third-party software before software/service become operational includes user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, software requirement specification, system configuration documents, system/database administrative documents, debugging/diagnostics documents, test procedures and results etc.</li> <li>•Necessary periodic updation/review (at least once in a quarter) of all the documents above must be carried out by the vendor and submitted to the bank.</li> <li>•Go-Live Payment will be linked to acceptance of Documents by the BANK</li> </ul> |
| Training                        | <ul style="list-style-type: none"> <li>•Training should be given by OEM</li> <li>•Core team training plan (functional &amp; technical)</li> <li>•Training manuals for core team training (functional &amp; technical)</li> <li>•End-user training manuals</li> </ul>  |
| Go Live                         | Go-live for all functionalities/ requirements as stated in the scope of work for the bidder including all features and circulars that NPCI and regulator have issued till Go-Live Date.   |

- vi) The team should report daily status to the Bank's IT head, or the person nominated for the rollout at the Bank's end.
- vii) Any deviation in the scheduled UAT plan has to be immediately communicated to the bank.
- viii) If required, the team has to work on Saturday's/ Sunday's and other non-working days to complete the task for the benefit of bank and quicker rollout.
- ix) Bidder team should co-ordinate with the Bank IT team whenever required for any input from the bank in regard to UAT, Bank will designate resources from IT team for the same.
- x) Bidder's team is responsible for preparing message dumps, logs, error-codes which are required by UPI and Bank team.
- xi) Bidder's Team is responsible for two rounds of comfort test and final UAT and sign-off from UPI UAT team.

### 5.17 Source Code:

- The application software should mitigate Application Security Risks, at a minimum; those discussed in OWASP top 10 (Open Web Application Security Project). The Bank shall have right to audit of the complete solution proposed by the bidder, and also inspection by the regulators of the country. The Bank shall also have the right to conduct source code audit by third party auditor.
- The Bidder shall provide complete and legal documentation of all subsystems, licensed operating systems, licensed system software, and licensed utility software and other licensed software. The Bidder shall also provide licensed software for all software products whether developed by it or acquired from others. The Bidder shall also indemnify the Bank against any levies / penalties on account of any default in this regard.
- In case the Bidder is coming with software, which is not its proprietary software, then the Bidder must submit evidence in the form of agreement it has entered into with the software vendor which includes support from the software vendor for the proposed software for the full period required by the Bank.

#### **5.18 Escrow arrangement:**

- Source code for customization done for Bank in UPI/IMPS Switch Solution and for other related services shall be provided by the Bidder to the Bank for unlimited and unrestricted use by the Bank. Bidder shall also provide all related material but not limited to flow charts, annotations, design documents schema, development, maintenance and operational tools and all related documentation.
- The core source code of the solutions in scope would be kept in escrow arrangement and complete information regarding the arrangement shall be provided by the bidder. Bidder shall transfer all Intellectual Property Right on non - exclusive basis for all the customizations done for Bank for the solutions and these IP rights would also be applicable for Bank's subsidiaries (Domestic).
- The Bank and the bidder shall appoint an escrow agent approved by the Bank to provide escrow mechanism for the deposit of the source code for the solution supplied/procured by the bidder to the Bank in order to protect the Bank's interests in an eventual situation.
- The Bank and the bidder shall enter into a tripartite escrow Agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent. As a part of the escrow arrangement, the bidder shall be required to provide a detailed code documentation which has been duly reviewed and certified by an external independent organization.
- The escrow code along with all documentation shall be periodically updated at-least once in a year or after Major changes by the bidder. Bidder shall submit a self-certificate confirming the same after every update.
- All costs for the Escrow arrangement will be borne by the Bank .

#### **5.19 Maintenance Support:**

The Bidder must provide uninterrupted availability of the system and ensure that the problem is resolved within the time schedule as prescribed in the Service Level Agreement (SLA). Maintenance support will also include installation of system updates and upgrades, providing corresponding updated manuals, and follow-up user training. During the contract period, all upgrades should be free. All regulatory / statutory changes should be done without any additional cost to the Bank.

### 5.20 Trainings:

The successful bidder shall provide a comprehensive training plan and study materials for designated bank officials who will manage the project during and after implementation, as advised by the Bank. The bidder shall ensure that the involved bank staff acquire knowledge of fundamental technologies related to application enabling them to effectively support and manage the deployed solutions. Necessary training sessions, including hands-on workshops and knowledge-sharing sessions, shall be conducted to equip bank staff with the required skills to operate and manage the solution/platform /application efficiently. The bank will inform the bidder annually about the number of bank staff requiring training, with a total of thirty candidates to be trained over the five-year contract period. All training-related activities shall be conducted by the bidder at their own expense, without any additional cost to the Bank.

## 6. Location of Work

The successful bidder shall be required to work in close co-ordination with Banks teams and may be required to work at different locations prescribed by Bank such as Banks DC/DR and other offices as per requirement. All expenses (travelling/lodging, etc.) shall be borne by the successful bidder. Implementation & Migration of the Project will be performed Onsite i.e. at Bank premises only. Comprehensive Project Plan along with minute sub-milestones of implementation and high level and low-level data flow diagrams should be shared with the Bank during kick-off meeting post issuance of purchase Order. Project Manager should be available ONSITE on all regular days and should update the project status on daily basis. The complete Implementation Team should also be stationed at Bank's location in Srinagar during all working days of Bank and if necessary, on holidays. The migration activity will be carried out during non-peak hours and Holidays. The successful bidder should provide enough resources to complete the project as per the timelines mentioned in the RFP document considering various dependencies on integrations with internal & external channels.

### 1. CHQ , Srinagar

Jammu & Kashmir Bank Ltd.  
Corporate Headquarters,  
MA Road, Srinagar-190001

### 2. Data Center Noida

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

**3. DR Mumbai**

CtrlS Data Center,  
Mahape, Navi Mumbai, Maharashtra , 400701

## 7. 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 ₹2500 by way of NEFT, details of which are mentioned at clause of Earnest Money Deposit in Part C.

1. Bidders are required to submit Earnest Money Deposit (EMD) for ₹70,00,000/- (Rupees Seventy Lac 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.
2. Technical Specifications, Price Bid, Terms and Conditions and various formats for submitting the tender offer are described in the tender document and Annexures.

## 8. Project Delivery Milestones

The solution as per the required scope needs to be rolled out as per the delivery timelines mentioned. The phases of the Schedule are as follows:

**PROJECT PHASES:**

1. Project Plan
2. Delivery of Solution
3. User Acceptance Testing
4. Operationalization of Solution
5. Solution Review

**1. PROJECT PLAN:**

Successful Bidder shall submit the project plan for complete implementation of the solution as per the Scope of Work detailed in this RFP along with Solution Architecture, DFD and other required documents. This plan should be submitted for review and bank's acceptance within two week after the issuance of PO to the successful bidder.

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

## 2. PROJECT MILESTONES & DELIVERY

The solution must be implemented as per project scope within a period defined in this RFP. Rollout of the solution has to be as per the below timelines:

| S.No | Milestone  | Timeline                            |
|------|--|-------------------------------------|
| 1    | Project Kick off Meeting   | Within 1 Week from issuance of PO   |
| 2    | Study of the existing system and GAP Analysis  | Within 3 Weeks from issuance of PO  |
| 3    | Requirement Analysis and Submission of SRS   | Within 5 Weeks from issuance of PO  |
| 4    | Deployment of application on new setup   | Within 8 Weeks from issuance of PO  |
| 5    | NPCI UPI Certification   | Within 20 Weeks from issuance of PO |
| 6    | UAT (testing & sign-off)   | Within 24 Weeks from issuance of PO |
| 7    | Migration of existing UPI/IMPS Data  | Within 28 Weeks from issuance of PO |
| 8    | Production movement and Pilot/ Closed User Group implementation followed by complete Go-live | Within 34 Weeks from issuance of PO |
| 9    | Project Signoff  | Within 36 Weeks from issuance of PO |

Successful bidder is expected to provide detailed project implementation status on weekly basis.

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:

- Claiming Liquidated Damages
- Termination of the purchase agreement fully or partly and claim liquidated damages.
- Forfeiting of Earnest Money Deposit / Invoking EMD Bank Guarantee/Performance Guarantee.

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

### EXTENSION OF DELIVERY SCHEDULE:

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

the Bank shall evaluate the situation and may at its discretion may extend the Bidder's time for performance against suitable extension of the performance guarantee for delivery.

**NON-DELIVERY:**

Failure of the successful bidder to comply with the above delivery schedule, shall constitute sufficient grounds for the annulment of the award of contract and invocation of bank guarantee (delivery) besides taking appropriate action against the successful bidder including blacklisting such bidder from participating in future tenders.

**3. USER ACCEPTANCE TESTING:**

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

**4. OPERATIONALIZATION OF SOLUTION:**

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

**5. REVIEW:**

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



## B-EVALUATION PROCESS

The endeavor of the evaluation process is to 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 **Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model**. 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 two stages, sequentially, as below:

### **Stage A. Evaluation of Eligibility**

### **Stage B: Technical Evaluation**

### **Stage C. Commercial Evaluation**

The three stage evaluation shall be done sequentially on knock-out basis. This implies that those Bidders qualifying in Stage A will only be considered for Stage B and those bidders 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.

### **Stage A-Evaluation of Eligibility**

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

### **Stage B-Evaluation of Technical Bid**



All technical bids of bidders who have Qualified Stage A will be evaluated in this stage and a technical score would be arrived at. The bidder should meet the technical requirements as mentioned in the Annexure F. 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.

**Bidders scoring at-least overall score of 70 marks or more as per Technical Bid Format in Annexure E ,will be declared technically qualified.**

Bank may seek clarifications from the any or each bidder as a part of technical evaluation. All clarifications received within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the Bank. Those Bidders who meet the threshold score of **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.

However, Bank reserves the right to relax the criteria but not less than **60%**.

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

## Stage C-Evaluation of Commercial Bid

### Cost Evaluation under Combined Quality cum Cost Based System (CQCCBS)

- i. Under CQCCBS, the technical proposals will be allotted weightage of 70% while the financial proposals will be allotted weightages of 30%.
- ii. Proposal with the lowest cost may be given a financial score of 100 and other proposals given financial scores that are inversely proportional to their prices
- iii. The total score, both technical and financial, shall be obtained by weighing the quality and cost scores and adding them up. The proposed weightages for quality and cost shall be specified in the RFP.

**Highest point's basis:**

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

As an example, the following procedure can be followed. In a particular case of selection of bidder, 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. In response to the RFP, 3 proposals, A,B & C were received. The technical evaluation committee awarded them 75, 80 and 90 marks respectively. The minimum qualifying marks were 65. All the 3 proposals were, therefore, found technically suitable and their financial proposals were opened after notifying the date and time of bid opening to the successful participants. The price evaluation committee examined the financial proposals and evaluated the quoted prices as under:

| Proposal | Technical Score | Evaluated cost |
|----------|-----------------|----------------|
| A        | 75              | Rs.120.        |
| B        | 80              | Rs.100.        |
| C        | 90              | Rs.110.        |

Using the formula  $LEC / EC$ , where LEC stands for lowest evaluated cost and EC stands for evaluated cost, the committee gave them the following points for financial proposals:

$$A : 100 / 120 = 83 \text{ points} \quad B : 100 / 100 = 100 \text{ points} \quad C : 100 / 110 = 91 \text{ points}$$

In the combined evaluation, thereafter, the evaluation committee calculated the combined technical and financial score as under:

$$\text{Proposal A: } 75 \times 0.70 + 83 \times 0.30 = 77.4 \text{ points.}$$

$$\text{Proposal B: } 80 \times 0.70 + 100 \times 0.30 = 80.9 \text{ points}$$

$$\text{Proposal C: } 90 \times 0.70 + 91 \times 0.30 = 87.9 \text{ points.}$$

The three proposals in the combined technical and financial evaluation were ranked as under:

Proposal A: 77.4 points : L3

Proposal B: 80.9 points : L2

Proposal C: 87.9 points : L1

Proposal C at the evaluated cost of Rs.110 was, therefore, declared as winner and recommended for negotiations/approval, to the competent authority.

.

## 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.abcpocure.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. 2,500/- 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<br>Srinagar J&K - 190001 |
| IFSC Code                 | JAKA0HRDCHQ   |
| Amount                    | INR 2,500/=   |

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 INR 70,00,000 (Rupees Seventy Lac 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<br>Srinagar J&K - 190001 |
| IFSC Code                              | JAKA0HRDCHQ   |
| Amount                                 | INR 70,00,000/=   |

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 F.

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:

|                 |   |
|-----------------|---|
| <b>Address:</b> | Technology & Development Department,<br>J&K Bank Ltd.<br>5 <sup>th</sup> Floor Corporate Headquarters,<br>MA Road Srinagar, J&K Pin- 190001 |
|-----------------|---|

**Note:** EMD is exempted for all Start-ups as recognized by DPIIT/DIPP. In case of such exemption, relevant documents/proof is to be submitted with Bid.

**The EMD made by the bidder will be forfeited if:**

- The bidder withdraws his tender before processing of the same.
- The bidder withdraws his tender after processing but before acceptance of the PO issued by Bank.
- The selected bidder withdraws his tender before furnishing an unconditional and irrevocable Performance Bank Guarantee.
- The bidder violates any of the provisions of the terms and conditions of this tender specification.

**The EMD will be refunded to:**

- The Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (other than Jammu & Kashmir Bank) from any scheduled commercial bank in India for 5% of the total project cost for 3 years and valid for 3 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.
- The Unsuccessful Bidder, only after acceptance of the PO by the selected 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 Purchase order cost for a period 3 years + 6 months. The format of the PBG is given as per **Annexure G**. 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 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. This contract will be awarded initially for a period of three (3) years from date of signing the contract & shall be further extended if both parties wish to continue on the mutually agreed terms and conditions.
- iv. If the service provided by the vendor is found to be unsatisfactory or if at any time it is found that the information provided by the vendor is false, the Bank reserves the right to revoke the awarded contract without giving any notice to the vendor. Bank's decision in this regard will be final.
- v. Bank will enter in to contract with the L1 bidder(s) (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 subject to Bank review. This includes changes in taxes or similar government decisions.
- 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. 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, Bank will have the right to allot those unfulfilled orders to other participating vendors, after giving 15-days" notice to the defaulting Vendor, provided the next vendor (L2) matches the rate fixed. 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 three parts:**

- a. Confirmation of Eligibility Criteria
  - b. Evaluation of Technical Bids
  - c. Commercial Bid" (CB).
- i. The mode of submission of Confirmation of Eligibility Criteria, Technical Bids and Commercial Bid (CB) shall be online.
  - ii. The Bidders who qualify the Eligibility Criteria will be qualified for technical bid evaluation. The successful Bidder(s) will be determined based as per the stated Commercial Evaluation process.
  - iii. Bidders are permitted to submit only one Bid and relevant Commercial Bid. More than one Bid should not be submitted.
  - iv. 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.
  - v. 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 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.
  - vi. All Schedules, Formats, Forms and Annexures should be stamped and signed by an authorized official of the bidder'
  - vii. 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.
  - viii. No rows or columns of the tender should be left blank. Offers with insufficient information are liable to rejection.
  - ix. 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.
  - x. 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.

- xi. Modification to the Bid Document, if any, will be made available as an addendum/corrigendum on the Bank's website and Online tendering portal.
- xii. 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.
- xiii. Prices quoted should be exclusive of GST.
- xiv. Applicable taxes would be deducted at source, if any, as per prevailing rates.
- xv. 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.
- xvi. 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.
- xvii. 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.
- xviii. 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 process shall remain valid for duration of 6 calendar months from the date of conclusion of RFP process
- iii. Once Purchase Order or Letter of Intent is issued by the Bank, the said price will remain fixed for the entire Contract period and shall not be subjected to variation on any account, including exchange rate fluctuations and custom duty. A Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

## 10. Bid Integrity

Willful misrepresentation of any fact within the Bid will lead to the cancellation of the contract without prejudice to other actions that the Bank may take. All the submissions, including any

accompanying documents, will become property of the Bank. The Bidders shall be deemed to license, and grant all rights to the Bank, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements.

## 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.

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

| S.No. | Project Milestone  | Payment (Incl. Of applicable taxes)  |
|-------|--|--|
| 1     | Successful Installation & setup at Hosted Location   | 10% of One Time Cost   |
| 2     | Successful Migration of Data   | 20% of One Time Cost   |
| 3     | 03 months after UAT Sign-off of platform and all regulatory Circulars & NPCI OC's circulars released up to 6 months from PO Date   | 30% of One Time Cost   |
| 4     | 03 months after Go-Live Sign-off of platform and all regulatory Circulars & NPCI OC's circulars released up to 6 months from PO Date                                     | 40% of One Time Cost   |
| 5     | Per Transaction Cost (Financial & Non-Financial) for UPI / IMPS/Merchant for Successful Transactions   | Monthly in arrears on submission of Invoices and required reports indicating the monthly successful transaction counts |
| 6     | Monthly Charges for Dedicated support team (Onsite) for L2/Product Manager Resources   | Quarterly As per Actuals   |
| 7     | Customization required for Bank ecosystem impacted by NPCI Circulars, RBI or regulatory requirement Change request excluding Platform/Switch related changes due to NPCI | Quarterly As per Actuals   |

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

- i) Post Signing of Service Level Agreement (SLA) & NDA between Bank and Successful bidder.
- ii) No advance payment will be made on award of the contract.
- iv) All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.
- v) Payments will be withheld in case of Non-compliance of the terms and condition of this RFP.

## 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 for implementation/support
- . 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 10 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 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, inclusive of all taxes and levies (excluding GST). 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 Company/Service Provider(including its sub-contractors).The Company shall be subject to annual audit by internal/ external Auditors appointed by the Bank / inspecting official from the RBI or the persons authorized by RBI or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and company is required to submit such certification by such Auditors to the Bank

Company shall allow the Bank and RBI or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Company within a reasonable time failing which Company will be liable to pay any charges/ penalty levied by the Bank

without prejudice to the other rights of the Bank. Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank."

## 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 of hereof may be amended or waived if, and only if such amendment or waiver is in writing and signed, in the case of an amendment by each Party, or in the case of a waiver, by the Party against whom the waiver is to be effective.

## 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 Jurisdiction 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 for **Implementation of Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model** and designated representative of the Bidder. If designated Officer of the Bank and representative of Bidder are unable to resolve the dispute within reasonable period, which in any case shall not exceed 30 days, they shall immediately escalate the dispute to the senior authorized personnel designated by the Bank and Bidder respectively. If even after elapse of reasonable period, which in any case shall not exceed 30 days, the senior authorized personnel designated by the Bank and Bidder are unable to resolve the dispute amicably OR any party fails to designate its officer/representative/ senior authorized personnel within 30 days from the date of request in writing for the same by the other party for amicable settlement of dispute, the same shall be referred to a sole arbitrator to be appointed by Bank. The Arbitration and Conciliation Act, 1996 will be applicable to the arbitration proceeding and the venue of the arbitration shall be at Srinagar. The language of the arbitration proceedings shall be in English. The award of the arbitrator shall be final and binding. The courts at Srinagar shall have exclusive jurisdiction at Srinagar.

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

### (NDA)

The Successful Bidder shall have to execute service level agreement for deliverables and successful execution of the projects to meet Banks requirement to its satisfaction. The Bank would stipulate strict penalty clauses for nonperformance or any failure in the implementation/efficient performance of the project .The Bidder should execute the Agreement within 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 shall follow J&K Bank's information security policy and instructions in this regard.
- c. The Successful Bidder acknowledges that J&K Bank 's business data and other proprietary information or materials, whether developed by J&K Bank or being used by J&K Bank pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to J&K Bank; and the Successful Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Successful Bidder to protect its own proprietary information. Successful Bidder recognizes that

the goodwill of J&K Bank depends, among other things, upon the Successful Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Successful

Bidder could damage J&K Bank. By reason of Successful Bidder's duties and obligations hereunder, Successful Bidder may come into possession of such proprietary information, even though the Successful Bidder does not take any direct part in or furnish the Service(s) performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by the Contract/Agreement. Successful Bidder shall use such information only for the purpose of performing the Service(s) under the Contract/Agreement.

- d. Successful Bidder shall, upon termination of the Contract/Agreement for any reason, or upon demand by J&K Bank, whichever is earliest, return any and all information provided to Successful Bidder by J&K Bank, including any copies or reproductions, both hardcopy and electronic.
- e. That the Successful Bidder and each of its subsidiaries have taken all technical and organizational measures necessary to protect the information technology systems and Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses. Without limiting the foregoing, the Successful Bidder and its subsidiaries have used reasonable efforts to establish and maintain, and have established, maintained, implemented and complied with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses.
- f. The Successful Bidder shall certify that to the knowledge of the Successful Bidder, there has been no security breach or other compromise of or relating to any information technology and computer systems, networks, hardware, software, data, or equipment owned by the Successful Bidder or its subsidiaries or of any data of the Successful Bidder's, the Operating Partnership's or the Subsidiaries' respective customers, employees, suppliers, vendors that they maintain or that, to their knowledge, any third party maintains on their behalf (collectively, "IT Systems and Data") that had, or would reasonably be expected to have had, individually or in the aggregate, a Material Adverse Effect, and
- g. That the Successful Bidder has not been notified of, and has no knowledge of any event or condition that would reasonably be expected to result in, any security breach or other compromise to its IT Systems and Data;
- h. That the Successful Bidder is presently in compliance with all applicable laws, statutes, rules or regulations relating to the privacy and security of IT Systems and Data and to the protection of such IT Systems and Data from unauthorized use, access, misappropriation or modification. Besides the Successful Bidder confirms the compliance with Banks Supplier Security Policy.
- i. That the Successful Bidder has implemented backup and disaster recovery technology consistent with generally accepted industry standards and practices.
- j. That the Successful Bidder and its subsidiaries IT Assets and equipment, computers, Systems,

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

- k. That the Successful Bidder shall be responsible for establishing and maintaining an information security program that is designed to:
  - Ensure the security and confidentiality of Customer Data, Protect against any anticipated threats or hazards to the security or integrity of Customer Data, and
  - That the Successful Bidder will notify Customer of breaches in Successful Bidder's security that materially affect Customer or Customer's customers. Either party may change its security procedures from time to time as commercially reasonable to address operations risks and concerns in compliance with the requirements of this section.
- l. The Successful Bidder shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of Personal Data and/or use, access, copying, exhibition, transmission or removal of Bank's Confidential Information from Companies facilities. Successful Bidder shall promptly provide Bank with written descriptions of such procedures and policies upon request. Bank shall have the right, upon reasonable prior written notice to Successful Bidder and during normal business hours, to conduct on-site security audits or otherwise inspect Companies facilities to confirm compliance with such security requirements.
- m. That Successful Bidder shall establish and maintain environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss or alteration of the Client Data, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are no less rigorous than those maintained by Successful Bidder for its own information or the information of its customers of a similar nature.
- n. That the Successful Bidder shall perform, at its own expense, a security audit no less frequently than annually. This audit shall test the compliance with the agreed-upon security standards and procedures. If the audit shows any matter that may adversely affect Bank, Successful Bidder shall disclose such matter to Bank and provide a detailed plan to remedy such matter. If the audit does not show any matter that may adversely affect Bank, Bidder shall provide the audit or a reasonable summary thereof to Bank. Any such summary may be limited to the extent necessary to avoid a breach of Successful Bidder's security by virtue of providing such summary.
- o. That Bank may use a third party or its own internal staff for an independent audit or to monitor the Successful Bidder's audit. If Bank chooses to conduct its own security audit, such audit shall be at its own expense. Successful Bidder shall promptly correct any deficiency found in a security audit.
- p. That after providing 30 days prior notice to Successful Bidder, Bank shall have the right to conduct a security audit during normal business hours to ensure compliance with the foregoing

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

- q. Successful Bidders are liable for not meeting the security standards or desired security aspects of all the ICT resources as per Bank's IT/Information Security / Cyber Security Policy. The IT /Information Security/ Cyber Security Policy will be shared with successful Bidder. Successful Bidders should ensure Data Security and protection of facilities/application managed by them.
- r. The deputed persons should aware about Bank's IT/IS/Cyber security policy and have to maintain the utmost secrecy & confidentiality of the bank's data including process performed at the Bank premises. At any time, if it comes to the notice of the bank that data has been compromised / disclosed/ misused/misappropriated then bank would take suitable action as deemed fit and selected vendor would be required to compensate the bank to the fullest extent of loss incurred by the bank. Besides bank will be at liberty to blacklist the bidder and take appropriate legal action against bidder.
- s. The Bank shall evaluate, assess, approve, review, control and monitor the risks and materiality of vendor/outsourcing activities and Successful Bidder shall ensure to support baseline system security configuration standards. The Bank shall also conduct effective due diligence, oversight and management of third party vendors/service providers & partners.
- t. Vendor criticality assessment shall be conducted for all partners & vendors. Appropriate management and assurance on security risks in outsources and partner arrangements shall be ensured.

## 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

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

## 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. 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.

## 29.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.

## 30.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.
- iv. The Bank shall if so required by applicable laws in force, at the time of payment, deduct income tax payable by the Successful Bidder at the rates in force, from the amount due to the Successful Bidder and pay to the concerned tax authority directly.

## Annexure A: Confirmation of Terms and Conditions

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

Dear Sir,

Sub: RFP No ..... for Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model , dated .....

Further to our proposal dated ....., in response to the Request for Proposal for Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model(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

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

Dear Sir,

Sub: RFP no: \_\_\_\_\_ for **Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model** dated \_\_\_\_\_

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer **Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model** 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 Bidder

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

| S. No. | PARTICULARS  | DETAILS |
|--------|--|---------|
| 1      | Name of the Company  |         |
| 2      | Postal Address   |         |
| 3      | Telephone / Mobile / Fax Numbers   |         |
| 4      | Constitution of Company  |         |
| 5      | Name & Designation of the Person Authorized to make commitments to the Bank    |         |
| 6      | Email Address  |         |
| 7      | Year of Commencement of Business   |         |
| 8      | Sales Tax Registration No  |         |
| 9      | Income Tax PAN No  |         |
| 10     | Service Tax / GST Registration No  |         |
| 11     | Whether OEM or System Integrator   |         |
| 12     | Name & Address of OEM/s.   |         |
| 13     | Brief Description of after sales services facilities available with the SI/OEM |         |
| 14     | Web Site address of the Company  |         |

Date:

Seal and signature of the bidder



### Annexure D: Compliance to Eligibility Criteria

The bidder needs to comply with all the eligibility criteria mentioned below. Non-compliance to any of these criteria would result in outright rejection of the Bidder's proposal. The bidder is expected to provide proof for each of the points for eligibility evaluation criteria. Any credential detail not accompanied by required relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

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

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

| S.No. | Eligibility Criteria   | Supporting Documents to be submitted  | Compliance (Y/N) |
|-------|--|---|------------------|
| 1     | The bidder should be a Government Organization/ PSU/ or a Limited Company / Private Limited Company under Company Act 1956/2013, India and should have been in existence for a minimum period of 5 years in India, as on date of submission of RFP.                                  | Certificate of Incorporation if it is company.  |                  |
| 2     | The firm should have an income tax PAN, GST No and the latest clearance certificate.   | Self-attested copies of PAN CARD, GST NO and latest income tax return to be submitted.            |                  |
| 3     | The bidder must have an annual turnover in India of INR 75 crores per annum in the last three financial years (i.e. 2021-22, 2022-23 and 2023-24) as per the audited balance sheet available at the time of submission of tender of individual company and not as group of companies | Copy of audited Balance Sheet and Certificate of the Chartered Accountant for preceding three FY. |                  |
| 4     | The bidder should have made operating profits in at least two financial years out of last three financial years (i.e. 2021-22, 2022-23 and 2023-24).   | Copy of audited Balance Sheet and Certificate of the Chartered Accountant for preceding three FY. |                  |
| 5     | The bidder should have positive net worth as per audited Balance sheet of the FY 2021-22, 2022-23 & 2023-24.   | P&L Statement of last 3 Financial years along with Auditor's certificate.                         |                  |

|    |  |   |  |
|----|--|---|--|
| 6  | The Bidder should have implemented the proposed UPI/IMPS solution and should be presently managing and providing services to at least two Scheduled Commercial Banks (SCB), out of which one Bank should have minimum average per day transaction of 1 Crore (including financial and non-financial) during last one year from April-24 to March-25. | Credential letter Along with<br>Proof of transactions.  |  |
| 7  | The Bidder should have implemented Merchant Acquisition Platform /Solution in at least 2 Banks as on date of publishing of RFP.  | Copy of the purchase / work order and Certificate of satisfactory completion of the Platform.   |  |
| 8  | The bidder should have implemented the proposed UPI/IMPS Solution(On Premise or Saas) in at least one Scheduled Commercial Bank having minimum 2000 Branches in India (SCB) and minimum per day transaction of 1 Crore, during last three year as on the date of submission of bid.  | The bidder has to provide relevant purchase order/work order / engagement letter & signoff along with satisfactory project completion certificate/ Reference letter from the Concerned Organization clearly stating the number of transactions. |  |
| 9  | The solution proposed by the Bidder should be certified by NPCI for implementation in any SC bank in India.  | Copy of the purchase / work order and satisfactory performance Certificate by any Scheduled Commercial Bank.  |  |
| 10 | Bidder/OEM should not have NPA with any Bank /financial institutions in India. Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Reserve Bank of India/NPCI to service the needs of the Bank   | Submit self-declaration on Company's letter head.   |  |
| 11 | At the time of bidding, the Bidder should not have been blacklisted/ debarred by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason or non-implementation/ delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.   | Submit the undertaking on Company's letter head   |  |

|    |  |  |  |
|----|--|--|--|
| 12 | At the time of bidding, there should not have been any pending litigation or any legal dispute in the last five years, before any court of law between the Bidder / OEM and the Bank regarding supply of goods/services.   | Submit the undertaking self-declaration on Company's letter head.  |  |
| 13 | If the bidder is from a country which shares a land border with India, the bidder should be registered with the Competent Authority  | Certified copy of the registration certificate   |  |
| 14 | The bidder and the solution offered should comply with all guidelines issued by RBI, NPCI etc. issued from time to time and should implement all such guidelines as and when required by regulatory bodies like NPCI/ NCIIPC /RBI/etc. without any additional cost to the Bank.  | A self-declaration to this effect is to be submitted on company's letter head.   |  |
| 15 | The solution should comply with Bank's Technical Specification at Annexure E1 & E2 & Service Provider Checklist (Annexure N).  | A self-declaration to this effect is to be submitted on company's letter head.   |  |
| 16 | The Bidder or Its Technology Partner should not be owned or controlled by any Director, Key managerial personnel, officer or employee of JKB or by related party having the same meaning as assigned under section 2(76) of the companies act or relative having same meaning as assigned section 2(77) of companies act 2013 read with rule 4 of the companies (specification of definition details rules 2014. | Undertaking to be given by the Bidder at time of submission compliance certificate given by successful bidder on company's letterhead (enclosed as Annexure 31) after signing agreement. |  |
| 17 | Bidder must have their DC (Primary) & DR (Secondary) for hosting proposed solution at different centres in India ideally falling under two seismic zones. These centres should be Tier-3 Data Centre or higher.  | Self-Declaration along with details of locations on bidder's letter head   |  |
| 18 | Bidder should be the Original Software Owner (OSO)/ Original Software Developer (OSD) of Solution.   | Letter of Undertaking in company's letter head has to submit in this effect.   |  |

|    |  |  |  |
|----|--|--|--|
| 19 | The bidder should have 24 X 7 Support centre in India.               | Details of Support Centre/ Undertaking on Letterhead of the Organizations.     |  |
| 20 | The Bidder should also comply with all guidelines set in Annexure-D1 | A self-declaration to this effect is to be submitted on company's letter head. |  |

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

1. Bidders need to ensure compliance to all the eligibility criteria points.
2. Purchase orders without relevant organization confirmation through a credential letter will not be considered as credentials.
3. Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory of the Bidder. Relevant portions, in the documents submitted in pursuance of eligibility criteria, should be highlighted.
4. Bank shall not consider the bids of bidders having poor or unsatisfactory past experience in execution or providing support to any project in past.
5. In case of mergers / acquisition / restructuring or name change, the date of establishment of the earlier / original partnership firm/limited company will be taken into account.
6. Providing any wrong information by the bidder will result in disqualification of the bidder. The Bank may cross check above parameters by any means / during site visit.
7. All Annexures must be on the letter head of the Bidder, except those which are to be provided by OEM/CA/third party.
8. All third party documents must be signed by their authorized signatory and his/her designation, Official E-mail ID and Mobile no. should also be evident. Bidder is also required to substantiate whether the person signing the document is authorized to do so on behalf of his company.

## **ANNEXURE -D1**

**Additional Explicit Clauses for Regulatory Compliance, Security  
Accountability, and Legal Ownership**

**1. Ownership and Legal Accountability Clause**

The Service Provider shall be solely responsible for end-to-end ownership of deployment, sustenance, uptime, operations, monitoring, and security of the UPI and IMPS solution hosted by the Service Provider (Whether On-Prem / Private or Public Cloud). The Service Provider shall ensure full compliance with all applicable Indian laws, All RBI Master Directions and Circulars applicable to the solution in particular and Information Security function in general (e.g., RBI Cyber Security Framework, Digital Payment Security Controls, Master Directions on IT Outsourcing Etc), NPCI operating circulars, IT Act (including amendments), and data protection mandates including but not limited to DPDP Act 2023. The provider shall be contractually bound to respond to all regulatory audits, inspections, and compliance directives at their own cost.

**2. Regulatory Compliance Assurance Clause**

The Service Provider shall certify compliance with regulatory requirements including but not limited to applicable RBI Guidelines, applicable NPCI guidelines, applicable CERT-In advisories, applicable NCIIPC critical infrastructure directives, and Data Localization requirements. Annual third-party compliance audits (e.g., PCI-DSS, ISO 27001, SOC 2, Substantive Architecture and Deployment Audit) must be conducted and shared with the Bank. The Service Provider must notify the Bank within 24 hours of any deviation or breach impacting compliance posture.

**3. Data Residency and Sovereignty Clause**

All data (including metadata, transaction data, PII, and logs) must reside and be processed only within Indian geographical boundaries. No data shall be stored, backed up, mirrored, or transferred outside India, even for redundancy or disaster recovery purposes, without prior written consent from the Bank.

**4. Security Governance & Certification Clause**

The Service Provider shall maintain valid and current certifications of ISO 27001, PCI-DSS, and CSA Certification for the underlying infrastructure. All application and infrastructure layers must be subject to continuous vulnerability management, security patching, and periodic VAPT testing. The results of all such tests must be made available to the Bank.

**5. Zero Trust Architecture and Log Integration Clause**

The Service Provider shall be fully responsible for the design, implementation, and operation of a security architecture based on Zero Trust principles, covering identity, access, network, workload, data, and application layers of the UPI/IMPS ecosystem hosted on the cloud.

The Service Provider shall ensure that all application and infrastructure-level logs, including authentication events, configuration changes, privilege escalations, API calls, and network traffic metadata, are collected, normalized, and retained in compliance with industry best practices and regulatory guidelines. These logs must be ingested into the Service Provider's own SIEM, PAM, and PIM solutions for threat detection, behavioural analysis, and incident response.

Additionally, the Service Provider shall ensure near real-time log streaming and integration of all relevant telemetry with the Bank's Cyber Security Operations Center (CSOC), SIEM, and PAM platforms using secure, standardized log formats and interfaces (e.g., syslog, JSON over TLS, RESTful APIs). The Bank shall have continuous visibility into the security state of the ecosystem, including the ability to conduct independent correlation, threat hunting, and audit of the data shared by the Service Provider.

The Service Provider shall ensure that the telemetry integration architecture enables bi-directional or federated alert sharing, so that any threats or anomalous behaviour detected by the Bank's monitoring infrastructure can be promptly escalated and remediated by the Service Provider.

All configurations, filters, and parsing logic used in log collection and forwarding must be documented and shared with the Bank, and the integration shall be reviewed and validated by the Bank prior to Go-Live. Failure to maintain secure and effective integration of security telemetry will be treated as a material breach of contract.

#### **6. Service Continuity and Exit Clause**

The Service Provider must ensure seamless transfer of services and data in a Bank-specified format in case of contract termination, regulatory instruction, or migration to another service provider/cloud. No proprietary locking shall be enforced that hinders portability.

#### **7. Cloud Security Posture Management (CSPM) Clause**

The Service Provider must implement and maintain continuous Cloud Security Posture Management using approved tools capable of detecting misconfigurations, exposure of sensitive data, and policy violations in real-time. Compliance dashboards must be accessible to the Bank. The Bank further reserves the right to monitor the cloud instance hosting Banks setup through its own CSPM tool set.

#### **8. Zero Downtime Security Patch Management Clause**

All critical and high severity security patches must be applied as per RBI, NPCI or CERT-In advisory timelines or in line with Bank's Vulnerability & patch Management procedures, and such patching must be performed with zero downtime using rolling updates, blue-green deployments, or other HA-compliant methods.

#### **9. Pre-Go-Live Audit and Conditional PO Clause**

The Bank reserves the right to conduct a comprehensive audit and review of the entire deployed infrastructure, including but not limited to cloud architecture, network components, security controls, access management configurations, data storage mechanisms, and application security posture, prior to the Go-Live of the UPI/IMPS solution.

The Service Provider shall provide full access to all environments, including Test, UAT, DC, DR, and staging setups, for this audit. Any deviations, gaps, or non-conformities observed during this audit or UAT period shall be documented and shared with the Service Provider.

If the Service Provider fails to rectify all reported issues within a fixed timeline mutually agreed between Bank and the Bidder, the Bank shall reserve the right to terminate the Purchase Order (PO) without any financial liability, revoke the Bank Guarantee and blacklist the vendor for future engagements.

This clause shall override all other contractual provisions related to delivery timelines, Go-Live acceptance, and partial compliance.

#### **10. Mandatory Third-Party Independent Infrastructure Audit Prior to Go-Live**

In addition to the Bank's right to conduct its own testing and audit of the deployed infrastructure, the Service Provider shall, at its own cost, ensure that a comprehensive third-party independent security audit and infrastructure review is conducted prior to the Go-Live of the UPI/IMPS solution.

This third-party audit shall cover, but not be limited to, the cloud hosting architecture, network design and segmentation, perimeter and internal security controls, access control mechanisms (including IAM, PAM), data storage and backup mechanisms, encryption practices, log management and monitoring configurations, container security, and application-level security posture.

The third-party auditor must be a CERT-In empanelled organization and must not be subcontracted by the Service Provider beyond a second level.

The final signed audit report with clear remarks on risk posture, compliance gaps (if any), and remediation status shall be submitted to the Bank at least 5 working days prior to the Bank's scheduled audit activity.

The Bank reserves the right to delay or defer its own audit or the Go-Live decision until this independent audit report is submitted and any significant gaps identified therein are addressed to the satisfaction of the Bank.



### Annexure E: Technical Bid Format

| S.No | Proposal Bid Evaluation   | Evaluation Parameters  | Max Marks |
|------|---|--|-----------|
| 1    | Total Number of Active Clients (Public Sector Banks & Private Sector Bank (Having more than 1000 branches) where UPI solution is implemented and running for last one year. | 1-2 Banks -5 Marks<br>3 Banks-8 Marks<br>>3 Banks -10 Marks  | 10 Marks  |
| 2    | Total Number of Active Clients (Public Sector Banks & Private Sector Bank Having more than 1000 branches) where IMPS solution is implemented and running for last one year. | 2 Banks -2 Marks<br>3 Banks-3 Marks<br>>3 Banks -5 Marks   | 5 Marks   |
| 3    | Total Number of UPI/IMPS Migrations carried out by bidder during the last 5 years   | 1 Migration:2 marks<br>2 Migrations:3 marks<br>>2 Migrations:5 marks   | 5 Marks   |
| 4    | Maximum No of UPI transactions (Financial & Non-Financial) handled by the Platform (Service Based Model) per day per bank for last one year.                                | 1-3 Crore Txns-3 Marks<br>3-5 Crore Txns-6 Marks<br>>5 Crore Txns-10 Marks   | 10 Marks  |
| 5    | Techno Functional Requirements  | Techno Functional Requirement<br>Annexure E-1 & Annexure E-2<br>Total 145 Point to be converted to equivalent of 20 Marks<br><br>Committee shall cross examine the compliance of the techno-functional | 20 Marks  |
| 6    | Demonstration of Live Solution showcasing Platform Features and Capability/Product Demonstration/ Technical Presentation/ Project Team Experience.                          | Committee Evaluation   | 30 Marks  |



|   |   |                      |                  |
|---|---|----------------------|------------------|
|   | Bidder(s) as part of technical evaluation have to demonstrate their Unified Payment Interface (UPI)/ IMPS solution. Bidder who fails in the demonstration will automatically stand disqualified in technical evaluation |                      |                  |
| 7 | Presentation showcasing the Methodology/ Approach & project execution/ implementation Plan  | Committee Evaluation | 10 Marks         |
| 8 | Compliance to Regulatory Circulars/Compliance Requirements (Annexure M) and Security Assessment/ Requirement (Annexure N)   | Committee Evaluation | 10 Marks         |
|   |   | <b>Total</b>         | <b>100 Marks</b> |

We hereby confirm that our proposed Solution meet all the specifications as mentioned above and have submitted the supporting documents against each point claimed. The bank reserves the right to ask the bidder to furnish any such document as required during technical evaluation.

Signature and Seal of Company

## Annexure E1: Technical Specifications

| Abbreviations | Full Form                                      | Marks |
|---------------|--|-------|
| A             | Available in the product without customization | 1     |
| C             | Will be provided with Customization            | 0.5   |
| N             | Not Available                                  | 0     |

| S.No.                             | Requirements  | A/C/N | Remark |
|-----------------------------------|---|-------|--------|
| <b>A-Application Architecture</b> |   |       |        |
| 1                                 | The architecture should support various banking delivery channels (current & future) such as Mobile, ATM, Payment Gateway, POS , QR Code , USSD, SMS, wearable etc.   |       |        |
| 2                                 | The architecture should support online real time updation between the application & database  |       |        |
| 3                                 | Integrity of the data should be maintained between the application & database.  |       |        |
| 4                                 | The architecture should have the ability to increase the number of concurrent instances to keep the application server parameters below 70% utilization (CPU, Memory, Hard disk, etc.)  |       |        |
| 5                                 | Application should be based on micro services architecture.   |       |        |
| 6                                 | Auto scalability - Ability to automatically scale horizontally in the event of spikes in volume, CPU, or memory utilization crossing threshold values.  |       |        |
| 7                                 | Application/Solution is platform agnostic - not dependent on a particular hardware setup  |       |        |
| 8                                 | Application/Solution is capable and being offered in such a manner that includes installation either as a single instance or multi instance depending on Bank's requirements  |       |        |
| 9                                 | Capable of being implemented on a Centralized, localized and /or a hub and spoke model Implementation 10.   |       |        |
| 10                                | Workflow based design for various applications and transaction originations & management.   |       |        |
| 11                                | It should Support <ul style="list-style-type: none"> <li>• Real time replication of data from Production site to Near Site to DC.</li> <li>• Should meet the Bank's RPO requirement for DR site.</li> <li>• Provide manual / automatic shift of the application to DR site</li> </ul> |       |        |

|    |  |  |  |
|----|--|--|--|
| 12 | Application/Solution architecture has the Capability to be configured in active-active mode in both DC and DRC.  |  |  |
| 13 | Application supports database and Server level Clustering  |  |  |
| 14 | Cloud Ready (Capability to host and move on private or public cloud)   |  |  |
| 15 | The proposed solution should be designable with MACH (micro services, API, cloud native and headless), scalable, plug and play, composable, modular, independent and loosely coupled architecture - The proposed solution should adhere to below design principles for micro services architecture |  |  |
| 16 | Each microservice should have independent development, testing, integration, and support capability  |  |  |
| 17 | Each microservice should have maximum reusability as well as separation of concerns  |  |  |
| 18 | Each microservices should offer isolation of environment, configuration variables, data etc., and allow communication only through APIs.   |  |  |
| 19 | Replication of data across microservices should not happen   |  |  |
| 20 | Each microservice should follow optimal design pattern per the business use case   |  |  |
| 21 | Each microservice should generate logs in a centralized repository to be used for monitoring, and not store any log locally  |  |  |
| 22 | Each microservice should integrate with centralized monitoring and performance telemetry tools   |  |  |
| 23 | Each microservice should be cloud native by design   |  |  |
| 24 | Each microservice should allow deployment as-is on premise, private cloud, or public cloud without design changes  |  |  |
| 25 | Microservices should support service discovery, service-mesh, and event streaming  |  |  |
| 26 | The successful bidder should procure and provide any tools and licenses required to support service discovery, service mesh, streaming / messaging etc.  |  |  |
| 27 | Leverage a container platform to build, host and run the microservices   |  |  |
| 28 | Underlying container platform should be compatible with on- premises, private cloud and public cloud installations   |  |  |

|    |  |  |  |
|----|--|--|--|
| 29 | Single control plane should cover all possible deployments (on- premises, private cloud, public cloud etc.), while control plane should be deployed in on-premises or private network only |  |  |
|----|--|--|--|

|    |  |  |  |
|----|--|--|--|
| 30 | The Application/Softwares should provide support to the underlying container platform like RedHat OpenShift, Vmware Tanzu, SUSE rancher etc. and other required software (like control plane, service mesh etc.)   |  |  |
| 31 | Be architected to be fault tolerant and ensure cascading failures do not occur   |  |  |
| 32 | Support graceful exception handling, restart, self-healing for UPI Switch- recovery process in the event of transaction or process failure   |  |  |
| 33 | Support native, hybrid-web, and web apps   |  |  |
| 34 | Ensure dynamic allocation of compute for load agnostic performance experience to customers   |  |  |
| 35 | Implement horizontal scalability at module/service level to handle required transaction volumes and composable architecture  |  |  |
| 36 | Guarantee 99.95% availability for the proposed solution  |  |  |
| 37 | Implement required integrations including core system integrations, partner, fintech and ecosystem integrations  |  |  |
| 38 | Implement caching across all digital channels appropriately, including static data caching, images, web assets (CSS, HTML, ICO etc.)   |  |  |
| 39 | Implement mature in-memory caching capabilities with cache store located nearest to the source of the provider in compliance with data storage requirements  |  |  |
| 40 | Implement configurable caching strategy based on type of data sources, consumers, data validity etc.   |  |  |
| 41 | Implement capability to push notifications regarding new changes over the air without frequent uploading on app store of various platforms.  |  |  |
| 42 | Implement highly scalable communication methods such as asynchronous APIs, event streaming and message queues where appropriate (e.g. user event-based triggers, data streaming pipelines, click-streaming analytics, mission-critical applications etc. |  |  |
| 43 | Implement standard optimization techniques (e.g.   |  |  |

|                                    |   |  |  |
|------------------------------------|---|--|--|
|                                    | caching, parallel processing, support standard optimization techniques, etc.)   |  |  |
| 44                                 | Leverage modern DevSecOps practices for faster and secure deployments of upgrades, patches and release management   |  |  |
| 45                                 | Leverage automated testing and performance testing to improve quality and speed of delivery.  |  |  |
| 46                                 | Ability to support for pooling multiple database connections when the load on the application increases   |  |  |
| <b>B-Software</b>                  |   |  |  |
| 47                                 | The Application should support IP V4 & V6 Hardware parameters (like CPU, Memory, hard-disk, NIC, etc.) should not cross the 70% utilization levels at any point in time.                            |  |  |
| 48                                 | Should be able to support different protocols (TCP/IP, IPX, etc.)   |  |  |
| 49                                 | Adequate staging procedures and test environments for staging should be supported   |  |  |
| 50                                 | Test software/application should be exactly same as production environment  |  |  |
| 51                                 | Software Solutions should be scalable to support increased requirements of the Bank   |  |  |
| 52                                 | Solution/Application should be platform agnostic. Page 111 of 147 RFP for UPI Switch- Tender No. GEM/2024/B/5670501   |  |  |
| 53                                 | Load/Stress/Performance reports are available for prescribed combination of OS, DB, Middleware & etc.   |  |  |
| <b>C-Availability Parameters</b>   |   |  |  |
| 54                                 | The solution should be available 24*7   |  |  |
| 55                                 | Automatic notification/reporting of application unavailability through mails, SMSs, etc.  |  |  |
| 56                                 | Automated Generation of Monthly availability report   |  |  |
| <b>D-Security / Data Integrity</b> |   |  |  |
| 57                                 | Integrity of data to be maintained at 100% of time  |  |  |
| 58                                 | Latest Encryption as per RBIs Digital Payment security be used for data traveling between core banking solution and delivery channels. i. Mention the encryption used in the Application /Solution. |  |  |
| 59                                 | Standards & Guidelines should be developed, implemented and followed for all IT assets  |  |  |
| 60                                 | Data Integrity should be ensured using internationally accepted hashing algorithms such as MD5  |  |  |
| 61                                 | System security is password controlled (for operating   |  |  |

|    |  |  |  |
|----|--|--|--|
|    | system, database, application and terminal id) which complies with the Bank's security policy (e.g. minimum password length, no. of attempts for login's, recycle of passwords etc.).  |  |  |
| 62 | Sensitive data such as passwords and authentication credentials shall not be logged in transaction or system activity files  |  |  |
| 63 | Successful and unsuccessful authentication attempts are logged   |  |  |
| 64 | Successful and unsuccessful authorization events are logged  |  |  |
| 65 | An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. In the event of interference, the Developer will ensure controls are in place to terminate the session and reverse out the affected transactions. As an integral part of the two-factor authentication architecture, appropriate measures to minimize exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack, are implemented |  |  |
| 66 | Sensitive information that is passed in the cookies is encrypted.  |  |  |
| 67 | The session identifier shall be random and unique.   |  |  |
| 68 | The session shall expire after a pre- defined length of time.  |  |  |
| 69 | The Service Provider shall create adequate controls ensuring that, when exception or abnormal conditions occur, resulting errors do not allow users to bypass security checks or obtain core dumps   |  |  |
| 70 | The Service Provider shall only install or use cryptographic modules based on authoritative standards and reputable protocols. The Service Provider shall implement strong cryptography and end- to-end application layer encryption to protect customer PINs, user passwords and other sensitive data in networks and storage. The Service Provider shall implement or support encryption when client account and transaction data is transmitted, transported, delivered or couriered to external parties or other Locations   |  |  |
| 71 | Security framework is supported in terms of authentication, multi-level authorization, auto log-   |  |  |

|                     |  |  |  |
|---------------------|--|--|--|
|                     | off, password control, single sign- on audit   |  |  |
| 72                  | System allows administrators to implement access management in a granular manner.  |  |  |
| 73                  | System provides comprehensive audit trail features to monitor activity of specific programs and data files etc. The system should also provide on-line access to audit trail information |  |  |
| 74                  | Time/date stamp, user ID, & before and after any changes in the system.  |  |  |
| 75                  | Activities executed by the Application system administrator  |  |  |
| 76                  | Segregation of duties is permitted (e.g. segregated function between system and application administration)  |  |  |
| 77                  | Ability to define groups so that access can be categorized   |  |  |
| <b>E-Interfaces</b> |  |  |  |
| 78                  | The system should be able to interface with the core banking system or any existing or future back office system online and seamlessly.  |  |  |
| 79                  | All modules in the system are fully integrated and provide online processing, real time updates and batch processing.  |  |  |
| 80                  | Solution is capable of being interfaced with multiple back offices simultaneously  |  |  |
| 81                  | Provision for an interface with the core banking solution, treasury solution, card management systems, payment processing systems, online channel, front- end customer portals, etc.     |  |  |
| 82                  | Provide support to XML, CSV, TXT, ISO, JSON etc. standard messaging protocols for interfacing.   |  |  |
| 83                  | Provide ability to define business rules for validation and translation of incoming messages   |  |  |
| 84                  | Ability to interface with email server. The system should support LDAP-s.  |  |  |
| 85                  | Interface protocols are supported e.g. ISO, XML etc. as required by NPCI.  |  |  |
| 86                  | Availability of application interface APIs on Unix and Windows platforms   |  |  |
| 87                  | Security features and consideration for the Interface - endto- end encryption  |  |  |
| 88                  | Interface able to handle exceptions (e.g. will output to log files, retries) when unsuccessful. Able to handle continual processing or gracefully terminated.                            |  |  |

|                              |   |  |  |
|------------------------------|---|--|--|
| 89                           | Interfaces support for both on-line and batch processing.   |  |  |
| 90                           | Starting & stopping the services/functionality through the admin portal   |  |  |
| 91                           | Offer isolation to microservices layer from the public facing API gateway layer. Inter-service communication should not take traffic out of the layer in which the services are hosted  |  |  |
| 92                           | Provide open APIs for integrations and conform to RESTful specifications  |  |  |
| 93                           | Ensure API caching is implemented wherever data refresh frequency is low  |  |  |
| 94                           | Provide APIs (with detailed documentation) for all omni channel digital banking platform capabilities to integrate with other systems   |  |  |
| 95                           | API specs should be maintained using industry standards such as Swagger/RAML and should be versioned along with the API's code or configuration   |  |  |
| 96                           | Support partner, fintech and ecosystem integrations through APIs, including catalog of digital services and APIs, automation features and accelerators for faster integration/onboarding, and other best in class open banking features |  |  |
| <b>F-Web Server</b>          |   |  |  |
| 97                           | The application should have the ability to support Apache, Netscape enterprise, Commerce server, Microsoft IIS, etc. as web servers   |  |  |
| 98                           | Should be able to install on UNIX flavors of Operating systems.   |  |  |
| 99                           | The web server should scale to future bank requirements   |  |  |
| <b>G- Application Server</b> |   |  |  |
| 100                          | The application should be able to support HTML, DHTML, etc. (Markup language)   |  |  |
| 101                          | Client-side scripting/ programming languages like Java scripts, VB scripts, Java Applets, ActiveX, etc. should be supported   |  |  |
| 102                          | The application should support the application layer technologies like Java, C++, Netscape server application process interface, Internet server application process interface, etc.  |  |  |
| 103                          | Database Connectivity support should at a minimum be ODBC, JDBC, etc.   |  |  |
| 104                          | Queuing system for prioritizing messages to external  |  |  |



|  |  |  |  |
|--|--|--|--|
|  | applications. The system should ensure the commit of the message.                    |  |  |
| 105  | Provide support for store-and-forward mechanism in case of a communication breakdown |  |  |
| 106  | Support standard queuing engines (IBM MQ, MSMQ, etc.)                                |  |  |
| <b>H-Archival, Purging and Restoration</b> |  |  |  |
| 107  | Application should capable to archive and retrieval of history transaction.          |  |  |
| 108  | Application/Solution should be capable to purge data.                                |  |  |
| 109  | Integrity of data during archival & purging  |  |  |
| 110  | Automated testing of backups   |  |  |



## Annexure E2: Functional Specifications

| Abbreviations | Full Form                                      | Marks |
|---------------|--|-------|
| A             | Available in the product without customization | 1     |
| C             | Will be provided with Customization            | 0.5   |
| N             | Not Available                                  | 0     |

| S.No.   | Requirements                                       | Mandatory/<br>Desired | A/C/N | Remark |
|---|--|-----------------------|-------|--------|
| <b>A-Experience of the Vendor</b>   |  |                       |       |        |
| 1   | Implementation of Admin Module                     | Mandatory             |       |        |
| 2   | Implementation of Merchant Onboarding Module       | Mandatory             |       |        |
| 3   | Implementation of Complaint Module                 | Mandatory             |       |        |
| 4   | Implementation of Bill Payment / Recharge facility | Mandatory             |       |        |
| 5   | Bulk Collection / Payment facility                 | Mandatory             |       |        |
| 6   | Single Debit / Multiple Credit facility            | Mandatory             |       |        |
| 7   | Self-onboarding of Merchant                        | Mandatory             |       |        |
| 8   | Recurring payment facility                         | Mandatory             |       |        |
| 9   | App intent facility                                | Mandatory             |       |        |
| 10  | Schedule Payment/Payment reminder facility         | Mandatory             |       |        |
| <b>B-Experience of the vendor related to following type of Merchant integration</b> |  |                       |       |        |
| 11  | Offline Merchant Integration                       | Mandatory             |       |        |
| 12  | Online Merchant Integration                        | Mandatory             |       |        |
| 13  | Integration with the E-commerce portal             | Mandatory             |       |        |
| 14  | Deep integration with Merchant /Wallet Mobile App  | Mandatory             |       |        |
| 15  | Integration with the chat platform                 | Mandatory             |       |        |
| 16  | Integration with the Bank's Mobile Banking Service | Mandatory             |       |        |



|    |  |           |  |  |
|----|--|-----------|--|--|
| 17 | Integration with POS/MPOS                            | Mandatory |  |  |
| 18 | Integration for providing POS facility using QR code | Mandatory |  |  |

**C-Experience related to Merchant integration for following type of transactions**

|    |                 |           |  |  |
|----|-----------------|-----------|--|--|
| 19 | P2B transaction | Mandatory |  |  |
| 20 | B2B transaction | Mandatory |  |  |
| 21 | P2G transaction | Mandatory |  |  |

**D-Audit Trail: Does the system provides comprehensive audit trail features such as:**

|    |   |           |  |  |
|----|---|-----------|--|--|
| 22 | Daily activities log are merged into the history log files  | Mandatory |  |  |
| 23 | Date, time and user-stamped transaction list are generated for different transactions   | Mandatory |  |  |
| 24 | Transaction screens display system information including Processing Date, Current Time, Current User                          | Mandatory |  |  |
| 25 | Daily activity reports are provided to highlight all the transactions being processed during the day                          | Mandatory |  |  |
| 26 | Support for recording of Unsuccessful attempts to login to the system   | Mandatory |  |  |
| 27 | System to provide session log files. The user should be able to analyze the information (e.g., account id, session time etc.) | Mandatory |  |  |
| 28 | System should provide tracking of the client's IP & Network Interface address   |           |  |  |

**E-Reporting**

|    |  |           |  |  |
|----|--|-----------|--|--|
| 29 | Provide a full set of operational and audit trail reports for each of the modules  | Mandatory |  |  |
| 30 | Periodical reports to appropriate authorities can be generated. The frequency and content of the reports can be determined by the bank user. | Mandatory |  |  |

|    |  |           |  |  |
|----|--|-----------|--|--|
| 31 | Generation / transmission of SMS/email alerts / advice at various stages of the transaction                        |           |  |  |
| 32 | Support for online access of reports   |           |  |  |
| 33 | Ensure complete log of all successful/unsuccessful events/accesses to the system/database by users, resources used | Mandatory |  |  |



|    |  |  |  |  |
|----|--|--|--|--|
|    | and actions performed (including recording all changed values where applicable) Automatic report generation capability |  |  |  |
| 34 | Pre-built query feature for non-Programmers  |  |  |  |
| 35 | Reports related to reconciliation & settlement   |  |  |  |

## Annexure F: Commercial Bid Format

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

| Description  | Unit Price in Rupees | Multiplication Factor (Tentative Qty) | Amount             |
|--|----------------------|---------------------------------------|--------------------|
| One time Implementation fee for end to end Solution on SaaS Based Model as per requirements mentioned under the RFP including migration          | a                    | 1                                     | A=a                |
| Per Transaction Cost (Financial & Non-Financial) of UPI / IMPS for SaaS Model (Cost Per Transaction in Rupees)- Year 1                           | b                    | 3,24,00,00,000                        | B=bx3,24,00,00,000 |
| Per Transaction Cost (Financial & Non-Financial) of UPI / IMPS for SaaS Model (Cost Per Transaction in Rupees)- Year 2 and Year 3                | c                    | 7,92,00,00,000                        | C=cx7,92,00,00,000 |
| One Time Migration Cost from SaaS Based Model to On-Prem model, if required by Bank<br><br>(Should include all OTC for Go-Live on On-Prem model) | d                    | 1                                     | D=d                |
| Per Transaction Cost (Financial & Non-Financial) of UPI / IMPS for On-Premise Model(Cost Per Transaction in Rupees)- Year 2 and Year 3           | e                    | 7,92,00,00,000                        | E=ex7,92,00,00,000 |
| Monthly Charges for Dedicated support team (Onsite) for L2/Product Manager Resources   | f                    | Resourcesx3<br>Yearsx12<br>Months     | F=fx1x36           |

|  |   |             |                  |
|--|---|-------------|------------------|
| Customization required for Bank ecosystem impacted by NPCI Circulars, RBI or regulatory requirement Change request excluding Platform/Switch related changes due to NPCI | g | 250 Mandays | $G=g \times 250$ |
| Network charges per annum  | h | 1           | $H=h \times 3$   |

|   |                   |
|---|-------------------|
| TCO for On Saas Based Model for 3 Years                             | $X = A+B+C+F+G+H$ |
| TCO for Hybrid Model for 3 Years (1year on SaaS and 2 Years OnPrem) | $Y=A+B+D+E+F+G$   |

**Note:**

- The transactions count is based on Assumption of 40% YOY growth as per current truncation value. Actual number may vary from the projected value and may be more than 40%.
- The Per Transaction Cost provided for SaaS and On-Prem models will be used for all Scenarios as depicted Below:
  - Scenario A:** Bank Continues to Host the Switch on all 3 Years on SaaS
  - Scenario B:** Bank uses the SaaS model for Year 1 and for Year 2 & 3 Bank switches to On-Prem or Bank's Private Cloud
  - Scenario C:** Bank uses the SaaS model for Year 1 & 2 & for Year 3 Bank switches to On-Prem or Bank's Private Cloud
- The per Transaction Cost for On-Prem model should be reasonably lower than SaaS costs ,with a minimum reduction of 30% on per transaction rate.
- Commercial Evaluation Process: L1 Bidder will be selected as per below process:
  - Single Bidder who has lowest TCO(X) and Lowest TCO(Y) will be **declared as L1**.
  - In case No Single Bidder has Lowest TCO in X & Y, the following Tie-Breaker will be used:  
Weighted Commercial Evaluation:  
TCO of SAAS Model (X): TCO of Hybrid Model (Y) = 60:40  
Calculation:  $TCO(X) * .60 + TCO(Y) * .40 = TCO (Z)$   
Bidder with lowest of TCO(Z) will be declared as L1

### Annexure G: Bank Guarantee Format

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 for **Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model.** (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 the RFP Document (which guarantee is hereinafter called as “BANK GUARANTEE”) AND WHEREAS the bidder has approached us, ..... for providing the BANK GUARANTEE.

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

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

1. We....., undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from you and undertake to indemnify you and keep you indemnified from time to time to the extent of Rs.....(Rupees .....only) an amount equivalent to the EMD against any loss or damage caused to or suffered by or that may be caused to or suffered by you on account of any breach or breaches on the part of the bidder of any of the terms and conditions contained in the RFP and in the event of the bidder commits default or defaults in carrying out any of the work or

discharging any obligation in relation thereto under the RFP or otherwise in the observance and performance of any of the terms and conditions relating thereto in accordance with the true intent and meaning thereof, we shall forthwith on demand pay to you such sum or sums not



exceeding the sum of Rs.....(Rupees..... only) as may be claimed by you on account of breach on the part of the bidder of their obligations in terms of the RFP. Any such demand made on the Bank shall be conclusive as regards amount due and payable by the Bank under this guarantee.

2. Notwithstanding anything to the contrary contained herein or elsewhere, we agree that your decision as to whether the bidder has committed any such default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you to establish your claim or claims under Bank Guarantee but will pay the same forthwith on your demand without any protest or demur.
3. This Bank Guarantee shall continue and hold good until it is released by you on the application by the bidder after expiry of the relative guarantee period of the RFP and after the bidder had discharged all his obligations under the RFP and produced a certificate of due completion of work under the said RFP and submitted a “ No Demand Certificate “ provided always that the guarantee shall in no event remain in force after the day of .....without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.
4. Should it be necessary to extend Bank Guarantee on account of any reason whatsoever, we undertake to extend the period of Bank Guarantee on your request under intimation to the SI/OEM till such time as may be required by you. Your decision in this respect shall be final and binding on us.
5. You will have the fullest liberty without affecting Bank Guarantee from time to time to vary any of the terms and conditions of the RFP or extend the time of performance of the RFP or to postpone any time or from time to time any of your rights or powers against the bidder and either to enforce or forbear to enforce any of the terms and conditions of the said RFP and we shall not be released from our liability under Bank Guarantee by exercise of your liberty with reference to matters aforesaid or by reason of any time being given to the bidder or any other forbearance, act or omission on your part of or any indulgence by you to the bidder or by any variation or modification of the RFP or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of so releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs.....( Rupees.....only ) as aforesaid or extend the period of the guarantee beyond the said day of ..... unless expressly agreed to by us in writing.

6. The Bank Guarantee shall not in any way be affected by your taking or giving up any securities from the bidder or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency or death as the case may be of the bidder
7. In order to give full effect to the guarantee herein contained, you shall be entitled to act as if we were your principal debtors in respect of all your claims against the bidder hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of Bank Guarantee.
8. Subject to the maximum limit of our liability as aforesaid, Bank Guarantee will cover all your claim or claims against the bidder from time to time arising out of or in relation to the said RFP and in respect of which your claim in writing is lodged on us before expiry of Bank Guarantee.
9. Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax or registered post to our local address as aforesaid and if sent accordingly it shall be deemed to have been given when the same has been posted.
10. The Bank Guarantee and the powers and provisions herein contained are in addition to and not by way of limitation of or substitution for any other guarantee or guarantees here before given to you by us (whether jointly with others or alone) and that Bank Guarantee is not intended to and shall not revoke or limit such guarantee or guarantees.
11. The Bank Guarantee shall not be affected by any change in the constitution of the bidder or us nor shall it be affected by any change in your constitution or by any amalgamation or absorption thereof or therewith but will ensure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.
12. The Bank Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.
13. We undertake to pay to you any money so demanded notwithstanding any dispute or disputes raised by the bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present being absolute and unequivocal.
14. The Bank Guarantee needs to be submitted in online form also via SFMS Application.
15. Notwithstanding anything contained herein above;

- i. our liability under this Guarantee shall not exceed Rs.....(Rupees.....only) ;
- ii. this Bank Guarantee shall be valid up to and including the date ..... and claim period shall be upto\_\_\_\_\_ ; and
- iii. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before the expiry of the claim period.

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

For and on behalf of BANK

Authorized Signatory

Seal

Address

## Annexure H: Performance Bank Guarantee Format

To

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 **Implementation of Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model** 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;

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

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

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

Dated the..... Day of .....2025.

For.....

BANK Authorized Signatory

## Annexure I: Non-disclosure Agreement (NDA)

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 vide Purchase Order No: \_\_\_\_\_ and each party may disclose or may come to know during the course of the project certain confidential technical and business information which the disclosing party desires the receiving party to treat as confidential.

**2. Confidential Information** means any information disclosed or acquired by other party during the course of the projects, either directly or indirectly, in writing, orally or by inspection of tangible objects (including without limitation documents, prototypes, samples, technical data, trade secrets, know-how, research, product plans, services, customers, markets, software, inventions, processes, designs, drawings, marketing plans, financial condition and the Company’s plant and equipment), which is designated as “Confidential,” “Proprietary” or some similar designation. Information communicated orally shall be considered Confidential Information if such information is confirmed in writing as being Confidential Information within a reasonable time after the initial disclosure. Confidential Information may also include information disclosed to a disclosing party by third parties. Confidential Information shall not, however, include any information which

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

- ii. becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party;
- iii. is already in the possession of the receiving party at the time of disclosure by the disclosing part as shown by the receiving party's files and records immediately prior to the time of disclosure;
- iv. is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality;
- v. is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as shown by documents and other competent evidence in the receiving party's possession; or
- vi. Is required by law to be disclosed by the receiving party, provided that the receiving party gives the disclosing party prompt written notice of such requirement prior to such disclosure and assistance in obtaining an order protecting the information from public disclosure.

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

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

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

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

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

Receiving Party shall immediately return and redeliver to Disclosing Party/ Bank all tangible material embodying the Confidential Information provided hereunder and all notes, summaries, memoranda, , records, excerpts or derivative information deriving there from and all other documents or materials (“Notes”) (and all copies of any of the foregoing, including “copies” that have been converted to computerized media in the form of image, data or word processing files either manually or by image capture) based on or including any Confidential Information, in whatever form of storage or retrieval, upon the earlier of (i) the completion or termination of the dealings between the parties contemplated hereunder; (ii) the termination of the Master Agreement; or (iii) at such time as the Disclosing Party/ Bank may so request.

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

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

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

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

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

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



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

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

The parties shall continue to be performing their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration. This agreement shall, in all respects, be governed by, and construed in accordance with the Laws of the UT of J&K read with applicable Laws of India. The Courts in Srinagar India shall have exclusive jurisdiction in relation to this agreement.

All notices or other communication under or in connection with this agreement shall be given in writing and may be sent by personal delivery, or post or courier or facsimile or email. Any such notice or other communication will be deemed to be effective if sent by personal delivery, when delivered, if sent by post, five days after being deposited in the post office and if sent by courier, three days after being deposited with the courier, if sent by facsimile, when sent (on receipt of a confirmation of having been sent to correct facsimile number) and if sent by 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**

By:\_\_\_\_\_

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

Title: \_\_\_\_\_

Address:\_\_\_\_\_

\_\_\_\_\_

Company Seal

**Bank**

By:\_\_\_\_\_

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

Title: \_\_\_\_\_

Address:\_\_\_\_\_

\_\_\_\_\_

Company Seal

## Annexure J: Service Level Agreement

This Service Level agreement (“Agreement”) is made at .....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:

### Definitions of the terms

|   |  |
|---|--|
| The Bank/J&K Bank:  | Reference to the “the Bank”, “Bank” and “Purchaser” shall be determined in context and may mean without limitation “Jammu & Kashmir Bank”. |
| Bidder/Vendor/Successful 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.  |
| SLA:  | This document in its entirety, inclusive of any addenda that may be issued by the Bank.  |
| The Contract:   | The agreement entered into between the Bank and the Company, as recorded in this Contract Form signed by the                               |

|                           |   |
|---------------------------|---|
|                           | parties, including all attachments and appendices thereto and all documents incorporated by reference therein.  |
| The Contract Price:       | The price payable to the Company under the Contract for the full and proper performance of its contractual obligations.   |
| The Product:              | All of the software or software, all hardware, database, middleware, operating systems and/or other materials which the Company is required to supply to the Bank under the Contract.   |
| System:                   | A Computer System consisting of all Hardware, Software, etc., which should work together to provide the services as mentioned in the Bid and to satisfy the Technical and Functional Specifications mentioned in the Bid.   |
| Specified Bank Location:  | Banks Data Centre located at Noida and Banks Disaster Recovery Site Located at Mumbai.  |
| PBG:                      | Performance Bank Guarantee.   |
| Material Breach:          | Company failure to perform a major part of this Agreement.  |
| Charges:                  | Commercials as per Purchase Order.  |
| Confidential Information: | It includes all types of Information that will be found on BANK systems that the Company may support or have access to including, but are not limited to, Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc. |

## Scope of Work

Vendor shall be responsible for providing services to Bank the Services defined the RFP for **Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model** in accordance with all the terms and conditions of the RFP clauses and as described in the Section 4 & Section 5 of A- Introduction of this RFP i.e **Brief Scope of work and Broad Scope of Work** respectively.

## Location of Work

The successful bidder shall be required to work in close co-ordination with Banks teams and may be required to work at different locations prescribed by Bank such as Banks DC/DR and other offices as per requirement. All expenses (travelling/lodging, etc.) shall be borne by the successful bidder. Implementation & Migration of the Project will be performed Onsite i.e. at Bank premises only. Comprehensive Project Plan along with minute sub-milestones of implementation and high level and low-level data flow diagrams should be shared with the Bank during kick-off meeting post issuance of purchase Order. Project Manager should be available ONSITE on all regular days and should update the project status on daily basis. The complete Implementation Team should also be stationed at Bank's location in Srinagar during all working days of Bank and if necessary, on holidays. The migration activity will be carried out during non-peak hours and Holidays. The successful bidder should provide enough resources to complete the project as per the timelines mentioned in the RFP document considering various dependencies on integrations with internal & external channels.

**1. CHQ , Srinagar**

Jammu & Kashmir Bank Ltd.  
Corporate Headquarters,  
MA Road, Srinagar-190001

**2. Data Center Noida**

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

**3. DR Mumbai**

CtrlS Data Center,  
Mahape, Navi Mumbai, Maharashtra , 400701

## Contract Uptime & Penalties

During Period of contract, Service Provider will maintain the services as per SLAs.

- i. Any bugs and enhancement in services shall be rectified immediately.
- ii. Any requirements amendments/modifications required by bank will have to be carried out by the identified Service Provider during the contract without any additional cost.
- iii. The maximum response time for a support/complaint from the site shall not exceed time defined, else it will fall under penalty clause.
- iv. Service Provider shall solve the software problem immediately after reporting of the problem by the Bank to the Service Provider.
- v. Any rectification required in the Application Software due to inherent bugs in the System Software/ off-the-shelf software shall also be rectified by the Service Provider, at no additional cost with timelines as defined in the SLA.

The Service Provider shall guarantee an uptime of 99.95% during the contract period which shall be calculated on Monthly basis. The "**Uptime**", for calculation purposes, equals to the Total

number of hours of the day in a month, less Downtime in number of hours. Any part of hour is treated as full hour.

- i. The "**Downtime**" is the time shall mean the time period when the Service/Application is not available as per the service standards of this SLA resulting failure. "**Failure**" is the condition that renders the solution not available to customers. "**Restoration**" is the condition when the Company demonstrates that the solution is in working order and the Bank acknowledges the same.
- ii. The percentage uptime is calculated on Monthly basis as follows:

$$\frac{(\text{Total hours in a month} - \text{downtime hours within the month})}{\text{Total hours in a month}} * 100$$

- iii. (A month is taken as a calendar month and number of days are actually number of days in each month)

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

|                   |        |
|-------------------|--------|
| Service Window    | 24*7   |
| Uptime Commitment | 99.95% |
| Data Availability | 100%   |

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

The percentage uptime is calculated on Monthly basis as follows:

$$\frac{(\text{Total hours in a month} - \text{downtime hours within the month})}{\text{Total hours in a month}} * 100$$

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

- b) The "**Downtime**" is the time shall mean the time period when the Service/Application is not available as per the service standards of this SLA resulting failure. "**Failure**" is the condition that renders the solution not available to customers. "**Restoration**" is the condition when the Company demonstrates that the solution is in working order and the Bank acknowledges the same.
- c) "**Percentage down time**" shall mean the aggregate of downtime of the particular system during the month expressed as a percentage of total available time in a year i.e. 90 \* 24 hours. Thus, if the aggregate downtime of System works out to 2 hours during a year then the percentage downtime shall be calculated as follows:

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

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

- d) **“Response Time”** shall mean the interval from receipt of first information from Bank to the company, or to the local contact person of the Company by way of any means of communication informing them of the malfunction in System/Solution to the time Company Engineer attends the problem.
- e) **“Restoration Time”** shall mean the period of time from the problem occurrence to the time in which the service returns to operational status. This may include temporary problem circumvention / workaround and does not necessarily include root cause removal.
- f) **“Resolution Time”** shall mean the period of time from the problem occurrence to the time in which the root cause of the problem is removed and a permanent fix has been applied to avoid problem reoccurrence.
- g) **Down Time”** shall mean the time period when the Service/Application is not available as per the service standards of this SLA, and the service/application is not available to the users of the Bank /Customers of the Bank ( and excludes the scheduled outages planned in advance IT infrastructure),due to the problem in it and downtime is the sum of response time and restoration time with the following exclusions:

Period when Bank denies access to the Company Engineer for carrying out repair activities.

During Period of contract, Service Provider will maintain the services as per SLAs. If the bidder fails to maintain guaranteed/committed uptime of 99.95% on monthly basis, Bank shall impose penalty as mentioned below on slab basis. In case the uptime falls below the levels as tabulated below, Bank shall impose a penalty for each percent of loss of uptime below the guaranteed level as per details below:

| Uptime         | Penalty/Month   |
|----------------|---|
| 99.95% & Above | NA  |
| 99.94% to 99%  | 3% of the Service Cost/Month  |
| 98.99% to 97%  | 5% of the Service Cost/ Month   |
| 97.99% to 95%  | 10% of the Service Cost/ Month  |
| Less than 95%  | Penalty at an incremental rate of 1% (in addition to a base of 10%) of the service cost for every 0.5% lower than the stipulated uptime |

Penalties shall also be applicable if the technical declines from the service provider are more than the threshold/ acceptable level of 1%.

| Technical declines | Penalty/Month |
|--------------------|---------------|
|--------------------|---------------|

|        |                                |
|--------|--------------------------------|
| 1%     | NA                             |
| >1%-3% | 2% of the Service Cost/Month   |
| >3-5%  | 3% of the Service Cost/ Month  |
| >5-8%  | 5% of the Service Cost/ Month  |
| >8-10% | 10% of the Service Cost/ Month |

Bank may recover such amount of penalty from any payment being released to the bidder, irrespective of the fact whether such payment is relating to this contract or otherwise. In case there is no pending invoices to be paid by the Bank to the bidder, the bidder has to submit a pay order / cheque payable at Srinagar in favour of Jammu & Kashmir Bank for the same within 15 days from the notice period from the Bank, failure of same may result in invoking of PBG for recovery of penalty. If the downtime exceeds 10 % and instances of downtime are more than 10 in a year, Bank has the discretion to cancel the contract.

If any penalty is levied by any regulator on the Bank which is attributed to the solution or any of its components, then the entire amount of such loss shall be recovered from the bidder on actual basis.

**Note: SLA will be monitored on monthly basis.**

#### **Service Levels:**

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Company shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the Company shall be reviewed by Bank that shall:

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

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

- Severity Level 1:** Is defined as, the Service is not available or there is a major degradation in performance of the system.
- Severity Level 2:** Is defined as, the service is available but the performance is degraded or there are intermittent failures and there is an urgent need to fix the problem to restore the service
- Severity Level 3:** Is defined as, the moderate degradation in the application performance. Has no impact on the normal operations/day-to-day working.

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



| Severity Level | Response | Restoration | Resolution |
|----------------|----------|-------------|------------|
| Severity-1     | 1 hrs.   | 2 hrs.      | 1 day      |
| Severity-2     | 1 hrs.   | 6 hrs.      | 2 days     |
| Severity-3     | 1 hrs.   | 12 hrs.     | 3 days     |

Penalties for Non Compliance to Restoration and Resolution Time:

| Severity Level | Restoration Breach  | Resolution Breach  |
|----------------|---|--|
| Severity-1     | 3 days of Service Cost/Month for every 3 hrs. of delay in restoration | 3 days of Service Cost/Month for every 1 day of delay in resolution  |
| Severity-2     | 3 days of Service Cost/Month for every 6 hrs of delay in restoration  | 3 days of Service Cost/Month for every 2 days of delay in resolution |
| Severity-3     | 3 days of Service Cost/Month for every 12 hrs delay in restoration    | 3 days of Service Cost/Month for every 5 days of delay in resolution |

#### Penalty for delayed Delivery:

Without prejudice to the rights of Bank to terminate this agreement/ the related purchase order, in case of the failure to deliver the solution/milestones within the stipulated timelines, penalty shall be levied for every 1 week delay beyond due date at the rate of 1% of the Total Implementation Cost (inclusive of all taxes, duties, levies etc ), up to a maximum of 10 weeks from the original delivery date .If delay exceeds 10 weeks, bank may in its sole discretion and without being bound to do so, extend the date of delivery or can invoke PBG and cancel the entire contract. In the event of the Bank agrees to extend the date of delivery at the request of the Company, it is a condition precedent that the validity of the Performance Bank Guarantee submitted by the Company in regard to the supply and maintenance etc. of the solution shall be extended by further period as required by the Bank before the expiry of the original Bank Guarantee. Failure to do so will be treated as breach of contract. Service Provider shall be excused of delay in case the installation could not be completed due to reasons not attributable to bidder, which shall be determined by Bank. Decision of Bank in this regard shall be final and binding.

#### Delivery & Installation:

The solution as per the required scope needs to be rolled out as per the delivery timelines mentioned. The phases of the Schedule are as follows:

##### PROJECT PHASES:

1. Project Plan
2. Delivery of Solution

3. User Acceptance Testing
4. Operationalization of Solution
5. Solution Review

## 1. PROJECT PLAN:

Successful Bidder shall submit the project plan for complete implementation of the solution as per the Scope of Work detailed in this RFP along with Solution Architecture, DFD and other required documents. This plan should be submitted for review and bank's acceptance within two week after the issuance of PO to the successful bidder.

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

## 2. PROJECT MILESTONES & DELIVERY

The solution must be implemented as per project scope within a period defined in this RFP. Rollout of the solution has to be as per the below timelines:

| S.No | Milestone  | Timeline                            |
|------|--|-------------------------------------|
| 1    | Project Kick off Meeting   | Within 1 Week from issuance of PO   |
| 2    | Study of the existing system and GAP Analysis  | Within 3 Weeks from issuance of PO  |
| 3    | Requirement Analysis and Submission of SRS   | Within 5 Weeks from issuance of PO  |
| 4    | Deployment of application on new setup   | Within 8 Weeks from issuance of PO  |
| 5    | NPCI UPI Certification   | Within 20 Weeks from issuance of PO |
| 6    | UAT (testing & sign-off)   | Within 24 Weeks from issuance of PO |
| 7    | Migration of existing UPI/IMPS Data  | Within 28 Weeks from issuance of PO |
| 8    | Production movement and Pilot/ Closed User Group implementation followed by complete Go-live | Within 34 Weeks from issuance of PO |
| 9    | Project Signoff  | Within 36 Weeks from issuance of PO |

Successful bidder is expected to provide detailed project implementation status on weekly basis.

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:

- d. Claiming Liquidated Damages
- e. Termination of the purchase agreement fully or partly and claim liquidated damages.
- f. Forfeiting of Earnest Money Deposit / Invoking EMD Bank Guarantee/Performance Guarantee.

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

#### **EXTENSION OF DELIVERY SCHEDULE:**

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

#### **NON-DELIVERY:**

Failure of the successful bidder to comply with the above delivery schedule, shall constitute sufficient grounds for the annulment of the award of contract and invocation of bank guarantee (delivery) besides taking appropriate action against the successful bidder including blacklisting such bidder from participating in future tenders.

#### **3. USER ACCEPTANCE TESTING:**

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

#### **4. OPERATIONALIZATION OF SOLUTION:**

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

#### **5. REVIEW:**

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

### **Contract Period**

The Contract shall be effective from date of acceptance of PO and shall be valid till (\_\_\_date\_\_\_), i.e 3 years from go live of the solution (\_\_\_date\_\_\_), unless or until terminated by Bank in accordance with the terms of this SLA. Thereafter the contract may further extended if both parties wish to continue on the mutually agreed terms and conditions subject to satisfactory performance of the vendor.

## Relocation and Shifting

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

## Payment Terms

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

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

| S.No. | Project Milestone  | Payment (Incl. Of applicable taxes)  |
|-------|--|--|
| 1     | Successful Installation & setup at Hosted Location   | 10% of One Time Cost   |
| 2     | Successful Migration of Data   | 20% of One Time Cost   |
| 3     | 03 months after UAT Sign-off of platform and all regulatory Circulars & NPCI OC's circulars released up to 6 months from PO Date   | 30% of One Time Cost   |
| 4     | 03 months after Go-Live Sign-off of platform and all regulatory Circulars & NPCI OC's circulars released up to 6 months from PO Date                                     | 40% of One Time Cost   |
| 5     | Per Transaction Cost (Financial & Non-Financial) for UPI / IMPS/Merchant for Successful Transactions   | Monthly in arrears on submission of Invoices and required reports indicating the monthly successful transaction counts |
| 6     | Monthly Charges for Dedicated support team (Onsite) for L2/Product Manager Resources   | Quarterly As per Actuals   |
| 7     | Customization required for Bank ecosystem impacted by NPCI Circulars, RBI or regulatory requirement Change request excluding Platform/Switch related changes due to NPCI | Quarterly As per Actuals   |

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

- i) Post Signing of Service Level Agreement (SLA) between Bank and Successful bidder.
- ii) Post Signing of Non-Disclosure Agreement (NDA) between Bank and Successful bidder.
- iii) No advance payment will be made on award of the contract.
- iv) All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.
- v) Payments will be withheld in case of Non-compliance of the terms and condition of this RFP.

**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.

**Entire Agreement, Amendments, Waivers.**

- i. This Master Agreement and each Service Attachment contains the sole and entire agreement of the parties with respect to the entire subject matter hereof, and supersede any and all prior oral or written agreements, discussions, negotiations, commitment, understanding , marketing brochures, and sales correspondence and relating thereto. In entering into this Master Agreement and each Service Attachment each party acknowledges and agrees that it has not relied on any express or implied representation, or other assurance (whether negligently or innocently made), out in this Master Agreement and each Service Attachment. Each party waives all rights and remedies which, but for this Section, might otherwise be available to it in respect of any such representation (whether negligently or innocently made), warranty, collateral contract or other assurance.
- ii. Neither this Master Agreement nor any Service Attachment may be modified or amended except in writing and signed by the parties.
- iii. No waiver of any provisions of this Master Agreement or any Service Attachment and no consent to any default under this Master Agreement or any Service Attachment shall be effective unless the same shall be in writing and signed by or on behalf of the party against whom such waiver or consent is claimed. No course of dealing or failure of any party to strictly enforce any term, right or condition of this Master Agreement or any Service Attachment shall be construed as a waiver of such term, right or condition. Waiver by either party of any default other party shall not be deemed a waiver of any other default.

**Severability**

If any or more of the provisions contained herein shall for any reason be held to be unenforceable in any respect under law, such unenforceability shall not affect any other provision of this Master

Agreement, but this Master Agreement shall be construed as if such unenforceable provisions or provisions had never been contained herein, provided that the removal of such offending term or provision does not materially alter the burdens or benefits of the parties under this Master Agreement or any Service Attachment.

### **Remedies Cumulative**

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

### **Partnership / Collaboration / Subcontracting**

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

### **Confidentiality**

All the Bank's product and process details, documents, data, applications, software, systems, papers, statements and business/customer information etc. (hereinafter referred to as 'Confidential Information') which may be communicated to or come to the knowledge of the Company and /or its employees during the course of discharging their obligations shall be treated as absolutely confidential and the Company and its employees shall keep the same secret and confidential and not disclose the same, in whole or in part to any third party nor shall use or allow to be used any information other than as may be necessary for the due performance by the Company of its obligations. The Company shall indemnify and keep Bank indemnified safe and harmless at all times against all or any consequences arising out of any breach of this undertaking regarding Confidential Information by the Company and/or its employees and shall immediately reimburse and pay to the Bank on demand all damages, loss, cost, expenses or any charges that Bank may sustain suffer, incur or pay in connection therewith.

It is clarified that "Confidential Information" includes any and all information that is or has been received by the Company (Receiving Party) from the Bank (Disclosing Party) and that (a) relates to the Disclosing Party and (b) is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed

information would be confidential (c) is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agent, representatives or consultants.

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

The Receiving Party, who receives the confidential information and the materials, agrees that on receipt of a written demand from the Disclosing Party, they will immediately return all written confidential information and materials and all copies thereof provided to and which is in Receiving Party's possession or under its custody and control.

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

The restrictions mentioned hereinabove shall not apply to:-

- (a) any information that publicly available at the time of its disclosure; or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same; or
- (b) any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any government, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosures, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.

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

The Company understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause BANK irreparable harm, may leave BANK with no adequate remedy at law and as such the Bank is entitled to proper indemnification for the loss caused by



the Company. Further the BANK is entitled to seek to injunctive relief besides other remedies available to it under law and this Agreement.

### Information Security:

- a. The 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:
  - o Ensure the security and confidentiality of Customer Data, Protect against any anticipated threats or hazards to the security or integrity of Customer Data, and
  - o That the Successful Bidder will notify Customer of breaches in Successful Bidder's security that materially affect Customer or Customer's customers. Either party may change its security procedures from time to time as commercially reasonable to address operations risks and concerns in compliance with the requirements of this section.
- l. The Successful Bidder shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of Personal Data and/or use, access, copying, exhibition, transmission or removal of Bank's Confidential Information from Companies facilities. Successful Bidder shall promptly provide Bank with written descriptions of such procedures and policies upon request. Bank shall have the right, upon reasonable prior written notice to Successful Bidder and during normal business hours, to conduct on-site security audits or otherwise inspect Companies facilities to confirm compliance with such security requirements.
- m. That Successful Bidder shall establish and maintain environmental, safety and facility procedures, data security procedures and other safeguards against the destruction,

corruption, loss or alteration of the Client Data, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are no less rigorous than those maintained by Successful Bidder for its own information or the information of its customers of a similar nature.

- n. That the Successful Bidder shall perform, at its own expense, a security audit no less frequently than annually. This audit shall test the compliance with the agreed-upon security standards and procedures. If the audit shows any matter that may adversely affect Bank, Successful Bidder shall disclose such matter to Bank and provide a detailed plan to remedy such matter. If the audit does not show any matter that may adversely affect Bank, Successful 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 Successful Bidder would be required to compensate the bank to the fullest extent of loss incurred by the bank.
- 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/Successful Bidders & partners.

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

## 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 90 days 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.

## Indemnity

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

- i. Intellectual Property infringement or misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.
- ii. Claims made by the employees who are deployed by the Successful bidder.
- iii. Breach of confidentiality obligations by the Successful bidder,
- iv. Negligence (including but not limited to any acts or omissions of the Successful bidder, its officers, principals or employees) or misconduct attributable to the Successful bidder or any of the employees deployed for the purpose of any or all of the its obligations,
- v. Any loss or damage arising out of loss of data;
- vi. Bonafide use of deliverables and or services provided by the successful bidder;
- vii. Non-compliance by the Successful bidder with applicable Laws/Governmental/Regulatory Requirements.

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

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

### Right to Audit

“Bank reserves the right to conduct an audit/ ongoing audit of the Company/Service Provider(including its sub-contractors).The Company shall be subject to annual audit by internal/ external Auditors appointed by the Bank / inspecting official from the RBI or the persons authorized by RBI or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and company is required to submit such certification by such Auditors to the Bank Company shall allow the Bank and RBI or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Company within a reasonable time failing which Company will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank’s documents by one or more officials or employees or other persons duly authorized by the Bank.”

### Limitation of Liability

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

## 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 one month during the contract period.

## Force Majeure

- i. The Selected Company shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.
- ii. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the 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 bidder 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

## Intellectual Property Rights

- 1.1 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.
- 1.2 Without the Bank's prior written approval, Company will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank's rights under this Agreement.
- 1.3 Company shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.
- 1.4 The Bank will give (a) notice to Company of any such claim without delay/provide reasonable assistance to Company in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Company shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Company shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Company shall consult with the Bank with respect to the defence and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses Of successful bidder
- 1.5 Company shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Company's compliance with the Bank's specific technical designs or instructions (except where Company knew or should have known that such compliance was likely to result in an Infringement Claim and Company did not inform the Bank of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

## Corrupt and Fraudulent practice.

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



- ii. “Corrupt Practice” means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.
- iii. “Fraudulent Practice” means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.
- iv. The Bank reserves the right to reject a proposal for award if it determines that the Company recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.
- v. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it becomes known that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

## Governing Laws and Dispute Resolution

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

The Bank and the 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 for **Implementation of Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model** 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.

## 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:

---

---

---

### Other Terms and Conditions

- i. If any provision of this agreement or any document, if any, delivered in connection with this agreement is partially or completely invalid or unenforceable in any jurisdiction, then that provision shall be ineffective in that jurisdiction to the extent of its invalidity or unenforceability. However, the invalidity or unenforceability of such provision shall not affect the validity or enforceability of any other provision of this agreement, all of which shall be construed and enforced as if such invalid or unenforceable provision was/were omitted, nor shall the invalidity or unenforceability of that provision in one jurisdiction affect its validity or enforceability in any other jurisdiction. The invalid or unenforceable provision will be replaced in writing by a mutually acceptable provision, which being valid and enforceable comes closest to the intention of the Parties underlying the invalid or unenforceable provision.
- ii. Bank reserves the right to conduct an audit/ ongoing audit of the services provided by Company. The Company agrees and undertakes to allow the Bank or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by the Company within a reasonable time failing which Bidder will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. The Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank.
- iii. The company, either by itself or through its group companies or Associates, shall not use the name and/or trademark/logo of Bank, in any sales or marketing publication or advertisement, or in any other manner.
- iv. Any addition, alteration, amendment, of this Agreement shall be in writing, signed by both the parties.



- v. The invalidity or unenforceability for any reason of any covenant of this Agreement shall not prejudice or affect the validity or enforceability of its other covenants. The invalid or unenforceable provision will be replaced by a mutually acceptable provision, which being valid and enforceable comes closest to the intention and economic positions of the Parties underlying the invalid or unenforceable provision.
- vi. Each party warrants that it has full power and authority to enter into and perform this Agreement, the respective executants are duly empowered and/or authorized to execute this Agreement, and performance of this Agreement will not result in breach of any provision of the Memorandum and Articles of Association or equivalent constitutional documents of the either party or any breach of any order, judgment or agreement by which the party is bound.
- vii. The terms and conditions laid down in the RFP shall be read and construed forming part of this service level agreement. In an event of contradiction on any term or condition between RFP and service level agreement, the terms and conditions of service level agreement shall prevail.

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

Agreed and signed on behalf of  
Company's Authorized Signatory

Name.....  
Designation.....

Witness (1):

Name.....  
Designation.....

Witness (2):

Name.....  
Designation.....

Agreed and signed on behalf of  
J&K Bank Limited

Name.....  
Designation.....

Witness (1):

Name.....  
Designation.....

Witness (2):

Name.....  
Designation.....

### Annexure K: Undertaking

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

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

Dear Sir,

Sub: RFP no: \_\_\_\_\_ for Selection of Service Provider for Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software) for Jammu and Kashmir Bank on Opex Model.

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer **Supply, Implementation, Migration and Maintenance of Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software)** 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, proposed to be followed by the Bank.

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

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

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

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

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

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

We enclose cost of RFP Rs.2,500/- (Two Thousand Five Hundred Only) and EMD of Rs.70,00,000/- (Rupees Seventy Lac 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 (KYE) Clause

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

1. We on the behalf of \_\_\_\_\_ (name of the company) hereby confirm that all the resources (both on-site and off-site) working on the Bank's project ie. **Supply, Implementation, Migration and Maintenance of Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software)**, 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 **Supply, Implementation, Migration and Maintenance of Unified Payment Interface (UPI) and Immediate Payment System (IMPS) Solution (Application & Software)**.

Sign and seal of Competent Authority  
Name of Competent Authority  
Dated

## Annexure M: Compliance Requirements

1. The solution should be in accordance with the security norms of RBI/NPCI/TRAI from time to time. The Regulatory mandates by any regulator pertaining to the application or solution provided by the bidder has to be complied during the validity of contract period without any extra cost to the Bank.
2. The solution proposed has to be in strict compliance with extant Laws and Regulations like but not limited to IT Act 2000 read with IT Amendment Act 2008, Draft Master Directions of RBI Directions on Outsourcing, RBI Digital Payment Security Directions 2021, TRAI, RBI Cyber Security Framework Circular Dated 2nd June 2016, NPCI Circulars and Directions.
3. As the Bank is opting for Managed Services Model, the bidder must ensure strict compliance with the Technology & Security Standards Viz, ISO 27001 ISMS or Equivalent Standard, ITIL Framework, DevSecOps, ISO 27018 Code of Practice for Personally Identifiable Information and other Software Development Standards.
4. The bidder shall ensure that a strong Project Governance Framework is put in place for adequately addressing associated risks and measuring the success of the project at any given point of time. The same needs to be communicated as part of the RFP response along with the escalation matrix.
5. In case the bidder opts for providing the services via a Multi-tenancy environment, it must be protected against data integrity and confidentiality risks and against co-mingling of data. The architecture should enable smooth recovery and any failure of any one or combination of components across the managed services architecture should not result in data/ information security compromise.
6. The Bidder shall share the appropriate update and release cycles affecting the service features (Such as: Security, Continuity, legal and governance...etc.). The bidder must be flexible to align the same with the Banks Patch, Vulnerability and Change Management Processes.
7. The Bidder, as part of bid submission shall share the detailed information on how the Service Provider ensures and applies agile and rapid yet comprehensive risk management. This must include the Risk Control checking Methodology.
8. In case the Service Provider is proposing the solution on Virtualized mode, the Service Provider has to ensure that the controls are in place to guarantee that only authorized snapshots are taken, and that these snapshots level of classification and storage location and encryption is compatible in strength with the production virtualization environment. Besides, the Service Provider has to ensure that the complete logs of Virtualized environment that are provided to Bank are accessible to Bank.
9. The bidder shall provide the Bank with its Service Providers user list that will have access to the Bank's data; at any point throughout the duration of the agreement. Service Providers should also update the Bank with any change in the employee list.
10. The bidder shall ensure to submit the high-level/low level design document as part of the solution offering mentioning integration of the application with Banks Privileged Identity and Access

Management Solution. The Bank shall be open to provide Identity Federated integration using SAML / OpenID / Open Auth, RADIUS etc.

11. The Admin & User Management Framework provided by the Service Provider must be in alignment with RBI's Authentication Framework for Customers, Privileged Accesses and other Internal Users.
12. The Service Provider must provide the Bank secure control for managing its identities (Including Identity Creation and Deletion / Modification & Termination).
13. The Service Provider shall ensure Authentication, Authorization, Accounting, Access control and logging (Format, retention and Access) meet the Bank's regulatory and legal requirements.
14. The Service Provider shall ensure that the logging is enabled for all activities including OS and, Application level for a period not less than 180 days online and then Backed up for the period of project. The Live logs as stipulated above shall as well be integrated with Bank's SIEM Solution.
15. The Service Provider shall have the information readily available on Location and time of access of the Service Provider Team.
16. The Service Provider shall ensure Micro-segmentation of Banks services. The Service Provider shall further shall ensure to put in place, in addition to the Infrastructure Security, the Application Layer Firewalls, conduct source code reviews prior to provisioning any application release, Adopt Secure web development best practices like OWASP secure development guidelines, Adopt OS and Applications security hardening best practices. Service Provider shall submit the source code audits reports mentioning closure of all identified vulnerabilities at yearly frequency to the Bank.
17. Service Provider shall ensure to conduct Periodic Vulnerability Assessment & Penetration testing of its Infrastructure and applications. The MPS shall ensure that these activities are done as part of Vulnerability Management and remediation program is defined, and it includes fixing the vulnerabilities based on priority. All vulnerabilities should be prioritized and must be fixed and patched within SLAs agreed upon by the Bank and the CSP in line with Banks Patch & Vulnerability Management procedure.
18. Service Provider shall ensure to follow a proper software development life cycle (SDLC) and that security is an integrated part in at least the following phases:
  - a. Planning and requirements gathering
  - b. Architecture and functional Design Phase Coding
  - c. Testing
  - d. Maintenance
19. The bidder shall ensure to adopt and is in compliance with Change Management and Incident Response Procedures as specified in (ITIL).
20. The Service Provider shall share its DR plan with Bank so as to ensure it matches the Bank's BCP requirements.
21. The Service Provider has the ability to retrieve and restore data following data loss incidents.

22. Service Provider to provide the Bank at least bi-annually with the DR testing reports. The reports should be comprehensive, covering from the exercise scope till the final outcome and recommendations.
23. Service Provider to ensure the DR solution is capable of maintaining the same levels of security measures and controls utilized in the normal operation mode.
24. Ensure that the DR solution is also owned and managed entirely by the Contracted Service Provider. Conducting DR Drills & DR compliances shall be the responsibility of Contracted Service Provider.
25. The Bidder shall ensure to meet the Maximum Time to Recover (MTTR) also known as RTO (Recovery Time Objective) of 3 Hours and Recovery Point Objective of Zero (0).
26. The Service Provider shall submit the data-segmentation and separation controls at each of the four main layers at the Service Provider: (1) Network, (2) physical, (3) system and (4) Application. The same must be kept updated and produced to the Bank as and when there are any changes or as sought by the Bank.
27. The bidder must be open for evaluation of each of the Data segmentation controls at each layer, as well as the number and type of controls at each layer every 6 months and after major system changes and upgrades.
28. The Service Provider shall ensure that data is encrypted at storage and in transit and in full compliance (at any given point in time) with Bank's Cryptographic Procedure, ISO 27001 and PCI-DSS Standard. The Databases must support the function of Encryption, Redaction/Masking and Comprehensive Audit Logging.
29. The Service Provider shall ensure that it is using a unique set of encryption key(s) for Bank. The unique encryption keys shall help protect data from being accessible in the event that it is inadvertently leaked from one Service Provider customer to another.
30. The Service Provider shall ensure to provide the "Exclusive" right to data ownership to the Bank throughout the duration of the agreement. The ownership includes all copies of data available with the Service Provider including backup media copies if any. The Service Provider is not permitted to use Bank's data for advertising or any other non-authorized secondary purpose.
31. The Service Provider shall contractually ensure that they inform the Bank "immediately" on any confirmed breach without any undue delay. The Service Provider shall ensure that Bank is notified within 4 hours of any "Suspected" breach from the time of breach discovery.
32. An "Exit Management Plan" must be put in place to define the rules of disengagement. Service Provider should provide the detailed description of the exit clause including agreed process, TAT for exit, data completeness and portability, secure purge of Bank's information, smooth transition of services, complete plan of how data shall be moved out from the hosted infrastructure with minimal impact on continuity of the Bank's operations.

33. It shall be responsibility of the service provider to ensure smooth transition of all the data of the Banks data including audit trails, logs, to Bank specified location/storage on the conclusion of services. It would be obligatory for the Service Provider not to delete any data without the written permission from the Bank.
34. Service Provider shall ensure to comply with the data and media destruction and sanitization controls as stipulated in Media Disposal and Sanitization Policies of Bank. The Service Provider shall further preserve documents as required by law and take suitable steps to ensure that Banks interests are protected, even post termination of the services. This would include ensuring full integrity data transition from service provider to alternate service provider or on premise setups.
35. The bidder shall ensure that the services are duly audited and certified by Cert-In Empaneled Audit Companies. The bidders are required to comply with requisite audit requirements as is specified under the security standards followed under the Information Technology Act and as stipulated by the Regulators from time to time.
36. Bank shall ensure that the Service Provider shall neither impede/ interfere with the ability of the Bank to effectively oversee and manage its activities nor impede the supervising authority in carrying out the supervisory functions and objectives.
37. The Service Provider shall ensure that the arrangement shall comply with all the policies of the Bank including, but not limit to, Information Security Policy, BCP, IT Outsourcing Policy, Incident Management Policy, etc. The service provider has to comply with all the laws/ regulations issued by RBI from time to time.
38. The Service Provider shall grant unrestricted and effective access to data related to the outsourced activities.
39. The relevant business premises of the Service Provider; subject to appropriate security protocols, for the purpose of effective oversight use by the Bank, their auditors, regulators and other relevant Competent Authorities, as authorized under law.
40. In case the technology/software platform/ hardware / infrastructure offered under the solution on hosted model reaches end of life / support during the contract period, the bidder has to ensure that the systems are either replaced or upgraded at their/bidders own cost without any disruption in the ongoing business transactions of the Bank.
41. Bidder shall not propose any solution/components which is near to end of life or end of support during the tenure of the contract.
42. The bidder has to ensure compliance with the Software Bill of Material (SBOM) issued by CERT-IN to manage potential risks, respond to security issues and comply with regulations. The bidder has to provide assurance regarding accuracy, completeness and timelines of SBOM.
43. The company shall comply to the Master Directions of RBI on IT outsourcing and bank's policy on IT Outsourcing with specifically on following points:



- i. *The service provide shall ensure that the Bank has an effective access to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity of the Bank, available with the service provider;*
- ii. *The service provider shall facilitate regular monitoring and assessment of the service provider by the Bank for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately;*
- iii. *The service provider shall inform the Bank about the material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to Bank to enable Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines;*
- iv. *The service provider shall ensure that the services being offered are in compliance with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data;*
- v. *The service provider shall ensure that storage of data (as applicable) is only in India as per extant regulatory requirements;*
- vi. *The service provider shall provide bank with details of data (related to Bank and its customers) captured, processed and stored;*
- vii. *The service provider shall not share any types of data/ information that the service provider (vendor) is not permitted to share with Bank's customer and / or any other party;*
- viii. *The Service provider shall have in place effective contingency plan(s) to ensure business continuity and testing requirements, in line with the Banks BCP;*
- ix. *Bank shall have right to seek information from the service provider about the third parties (in the supply chain) engaged by the former;*
- x. *The service provider shall be contractually liable for the performance and risk management practices of its sub-contractors;*
- xi. *It shall be obligation of the service provider to comply with directions issued by the RBI in relation to the activities outsourced to the service provider, through specific contractual terms and conditions specified by the Bank;*
- xii. *It shall be obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the Bank;*
- xiii. *There shall be a provision to consider skilled resources of service provider who provide core services as "essential personnel" so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations);*
- xiv. *The service provider should have a suitable back-to-back arrangements with the concerned OEM, if applicable*

### Annexure N: Hosting Assessment Checklist

|  | Control Domain     | CID   | SP Assessment Questions  | Requirement | Answer (Yes/No) | Reference |
|--|--------------------|-------|--|-------------|-----------------|-----------|
|  |                    | CO.01 | *Do you allow customers to view your third party audit reports?  | Mandatory   |                 |           |
|  |                    | CO.02 | *Do you conduct network penetration tests of your service infrastructure regularly? If yes please elaborate on your test and remediation process                                     | Mandatory   |                 |           |
|  |                    | CO.03 | *Do you conduct regular application penetration tests of your infrastructure according to the industry best practices? If yes please elaborate on your test and remediation process. | Mandatory   |                 |           |
|  |                    | CO.04 | *Do you conduct internal audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.                                    | Mandatory   |                 |           |
|  |                    | CO.05 | *Do you conduct external audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.                                    | Mandatory   |                 |           |
|  |                    | CO.06 | Are the results of the network penetration tests available to customers at their request?  |             |                 |           |
|  |                    | CO.07 | *Are the results of internal and external audits available to customers at their request?  | Mandatory   |                 |           |
|  | Third Party Audits | CO.08 | Do you permit customers to perform independent vulnerability assessments?  |             |                 |           |

|                        |                                       |       |  |           |  |  |
|------------------------|---------------------------------------|-------|--|-----------|--|--|
| INFORMATION GOVERNANCE | Contact / Authority Maintenance       | CO.9  | Do you maintain updated liaisons and points of contact with local authorities? If yes then how frequently you validate the contacts?   |           |  |  |
|                        | Information System Regulatory Mapping | CO.10 | *Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single customer only, without inadvertently accessing another customer's data? | Mandatory |  |  |
|                        |                                       | CO.11 | *Do you have capability to logically segment, isolate and recover data for a specific customer in the case of a failure or data loss?  | Mandatory |  |  |
|                        | Intellectual Property                 | CO.12 | *Do you have policies and procedures in place describing what controls you have in place to protect customer's data marked as intellectual property?                                       | Mandatory |  |  |
|                        |                                       | CO.13 | If utilization of customers services housed is mined for provider benefit, are the customers' defined IP rights preserved?   |           |  |  |
|                        |                                       | CO.14 | If utilization of customers services housed is mined for provider benefit, do you provide customers the ability to opt-out?  |           |  |  |
| INFORMATION GOVERNANCE | Ownership                             | IG.01 | *Do you follow or support a structured data-labelling standard (ex. ISO 15489, Oasis XML Catalogue Specification,  | Mandatory |  |  |

|                           |  |       |  |           |  |  |
|---------------------------|--|-------|--|-----------|--|--|
| INFORMATION<br>GOVERNANCE |  |       | CSA data type guidance)? If yes please specify   |           |  |  |
|                           | Classification                         | IG.02 | Do you provide a capability to identify virtual machines via policy tags/metadata?   |           |  |  |
|                           |  | IG.03 | Do you provide a capability to identify hardware via policy tags/metadata/hardware tags?   |           |  |  |
|                           |  | IG.04 | Do you have a capability to use system geographic location as an authentication factor?  |           |  |  |
|                           |  | IG.05 | *Can you provide the physical location/geography of storage of a customer's data upon request?   | Mandatory |  |  |
|                           |  | IG.06 | *Do you allow customers to define acceptable geographical locations for data routing or resource instantiation?  | Mandatory |  |  |
|                           | Handling / Labelling / Security Policy | IG.07 | Do you consider all customer data to be "highly sensitive "and provide the same protection and controls across the board or you apply the controls according to the data specific classification or label? |           |  |  |
|                           |  | IG.08 | *Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?   | Mandatory |  |  |
| INFORMATION<br>GOVERNANCE | Retention Policy                       | IG.09 | *Do you have technical control capabilities to enforce customer data retention policies?   | Mandatory |  |  |
|                           |  | IG.10 | *Do you have a documented procedure for responding to  | Mandatory |  |  |

|                        |                     |       |   |           |  |  |
|------------------------|---------------------|-------|---|-----------|--|--|
|                        |                     |       | requests for customer data from governments or third parties?   |           |  |  |
|                        | Secure Disposal     | IG.11 | *Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the customer?   | Mandatory |  |  |
|                        |                     | IG.12 | *Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of customer data once a customer has exited your environment or has vacated a resource? | Mandatory |  |  |
|                        | Nonproduction Data  | IG.13 | *Do you have procedures in place to ensure production data shall not be replicated or used in your test environments?   | Mandatory |  |  |
|                        | Information Leakage | IG.14 | *Do you have controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-customer environment?  | Mandatory |  |  |
|                        |                     | IG.15 | Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your service offering?  |           |  |  |
| <b>PHYSICAL ACCESS</b> | Policy              | PA.01 | *Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?  | Mandatory |  |  |

|  |                            |       |  |           |  |  |
|--|----------------------------|-------|--|-----------|--|--|
|  | User Access                | PA.02 | *Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background checks?  | Mandatory |  |  |
|  | Controlled Access Points   | PA.03 | *Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?                       | Mandatory |  |  |
|  | Secure Area Authorization  | PA.04 | *Do you allow customers to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)? | Mandatory |  |  |
|  | Unauthorized Persons Entry | PA.05 | *Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?                      | Mandatory |  |  |
|  | Offsite Authorization      | PA.06 | Do you provide customers with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)            |           |  |  |
|  | Offsite equipment          | PA.07 | Do you provide customers with documentation describing your policies and procedures  |           |  |  |

|  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|
|  |  |  | governing asset management and repurposing of equipment? |  |  |  |
|--|--|--|--|--|--|--|

|                      |                                  |       |   |           |  |  |
|----------------------|----------------------------------|-------|---|-----------|--|--|
|                      | Asset Management                 | PA.08 | *Do you maintain a complete inventory of all of your critical assets?   | Mandatory |  |  |
| HR                   | Employment Agreements            | HR.01 | *Do you specifically train your employees regarding their role vs. the customer's role in providing information security controls?  | Mandatory |  |  |
|                      |                                  | HR.02 | Do you document employee acknowledgment of training they have completed?  |           |  |  |
|                      | Employment Termination           | HR.03 | *Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?   | Mandatory |  |  |
| INFORMATION SECURITY | Management Program               | IS.01 | *Do you provide customers with documentation describing your Information Security Management System (ISMS)?   | Mandatory |  |  |
|                      | Management Support / Involvement | IS.02 | *Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution? | Mandatory |  |  |
|                      | Policy                           | IS.03 | Do your information security and privacy policies align with particular standards (ISO-27001, NIA, CoBIT, etc.)?  |           |  |  |

|  |  |       |  |  |  |  |
|--|--|-------|--|--|--|--|
|  |  | IS.04 | Do you have agreements which ensure your providers adhere to your information security and privacy policies? |  |  |  |
|--|--|-------|--|--|--|--|

|                      |                       |       |   |           |  |  |
|----------------------|-----------------------|-------|---|-----------|--|--|
|                      |                       | IS.05 | *Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?                                    | Mandatory |  |  |
|                      | Baseline Requirements | IS.06 | *Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)? | Mandatory |  |  |
|                      |                       | IS.07 | Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?                      |           |  |  |
|                      |                       | IS.08 | *Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?                                | Mandatory |  |  |
|                      | Policy Reviews        | IS.09 | Do you notify your customers when you make material changes to your information security and/or privacy policies?   |           |  |  |
| INFORMATION SECURITY |                       | IS.10 | *Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?  | Mandatory |  |  |
|                      |                       | IS.11 | *Are employees made aware of what action might be taken in the event of a violation and   | Mandatory |  |  |



|  |   |       |   |           |  |  |
|--|---|-------|---|-----------|--|--|
|  |   |       | stated as such in the policies and procedures?  |           |  |  |
|  | User Access Policy                      | IS.12 | *Do you have controls in place ensuring timely removal of access rights and permissions which is no longer required?  | Mandatory |  |  |
|  |   | IS.13 | *Do you provide metrics which track the speed with which you are able to remove access rights following a request from us?  | Mandatory |  |  |
|  | User Access Restriction / Authorization | IS.14 | *Do you document how you grant and approve access to customer data?   | Mandatory |  |  |
|  |   | IS.15 | Do you have a method of aligning provider and customer data classification methodologies for access control purposes?   |           |  |  |
|  | User Access Revocation                  | IS.16 | *Is timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties? | Mandatory |  |  |
|  | User Access Reviews                     | IS.17 | *Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your customers)?  | Mandatory |  |  |
|  |   | IS.18 | *If users are found to have inappropriate entitlements, are   | Mandatory |  |  |

|  |  |  |   |  |  |  |
|--|--|--|---|--|--|--|
|  |  |  | all remediation and certification actions recorded? |  |  |  |
|--|--|--|---|--|--|--|

|  |                                   |       |   |           |  |  |
|--|-----------------------------------|-------|---|-----------|--|--|
|  |                                   | IS.19 | Will you share user entitlement remediation and certification reports with your customers, if inappropriate access may have been allowed to customer data?  |           |  |  |
|  | Training / Awareness              | IS.20 | *Do you provide or make available a formal security awareness training program access and data management issues (i.e., multi-tenancy, nationality, delivery model segregation of duties implications, and conflicts of interest) for all persons with access to customer data? | Mandatory |  |  |
|  |                                   | IS.21 | *Are administrators properly educated on their legal responsibilities with regard to security and data integrity?   | Mandatory |  |  |
|  | Industry Knowledge / Benchmarking | IS.22 | Do you participate in industry groups and professional associations related to information security?  |           |  |  |
|  |                                   | IS.23 | *Do you benchmark your security controls against industry standards?  | Mandatory |  |  |
|  | Roles / Responsibilities          | IS.24 | Do you provide customers with a role definition document clarifying your administrative responsibilities vs. those of the customer?   |           |  |  |

|                      |                              |       |  |           |  |  |
|----------------------|------------------------------|-------|--|-----------|--|--|
|                      | Managem<br>ent<br>Oversight  | IS.25 | Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?                          |           |  |  |
| INFORMATION SECURITY | Segregati<br>on of<br>Duties | IS.26 | Do you provide customers with documentation on how you maintain segregation of duties within your service offering?  |           |  |  |
|                      | User<br>Responsi<br>bility   | IS.27 | *Is your staff made aware of their responsibilities for maintaining awareness and compliance with our published security policies, procedures, standards and applicable regulatory requirements? | Mandatory |  |  |
|                      |                              | IS.28 | Are users made aware of their responsibilities for maintaining a safe and secure working environment?  |           |  |  |
|                      |                              | IS.29 | Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?  |           |  |  |
|                      | Workspac<br>e                | IS.30 | *Do your data management policies and procedures address customer and service level security requirements?   | Mandatory |  |  |
|                      |                              | IS.31 | Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to customer data?  |           |  |  |
|                      |                              | IS.32 | *Does the virtual machine management infrastructure include a tamper audit or  | Mandatory |  |  |

|  |                                |       |  |           |  |  |
|--|--------------------------------|-------|--|-----------|--|--|
|  |                                |       | software integrity function to detect changes to the build/configuration of the virtual machine?   |           |  |  |
|  | Encryption                     | IS.33 | *Do you have a capability to allow creation of unique encryption keys per customer?  | Mandatory |  |  |
|  |                                | IS.34 | Do you support customer generated encryption keys or permit customers to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)? |           |  |  |
|  | Encryption Key Management      | IS.35 | *Do you encrypt customer data at rest (on disk/storage) within your environment?   | Mandatory |  |  |
|  |                                | IS.36 | *Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?                                      | Mandatory |  |  |
|  |                                | IS.37 | Do you have a capability to manage encryption keys on behalf of customers?   |           |  |  |
|  |                                | IS.38 | Do you maintain key management procedures?   |           |  |  |
|  | Vulnerability/Patch Management | IS.39 | *Do you conduct network-layer vulnerability scans regularly?   | Mandatory |  |  |
|  |                                | IS.40 | *Do you conduct application-layer vulnerability scans regularly?   | Mandatory |  |  |

|                      |                                |       |   |           |  |  |
|----------------------|--------------------------------|-------|---|-----------|--|--|
|                      |                                | IS.41 | *Do you conduct local operating system-layer vulnerability scans regularly?   | Mandatory |  |  |
|                      |                                | IS.42 | *Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?   | Mandatory |  |  |
| INFORMATION SECURITY |                                | IS.43 | Will you provide your risk- based systems patching timeframes to your customers upon request?   |           |  |  |
|                      | Antivirus / Malicious Software | IS.44 | Do you deploy multi anti-malware engines in your infrastructure?  |           |  |  |
|                      |                                | IS.45 | Do you ensure that security threat detection systems which use signatures, lists, or behavioural patterns are updated across all infrastructure components within industry accepted timeframes? |           |  |  |
|                      | Incident Management            | IS.46 | *Do you have a documented security incident response plan?  | Mandatory |  |  |
|                      |                                | IS.47 | Do you integrate customized customer requirements into your security incident response plans?   |           |  |  |
|                      |                                | IS.48 | Do you have a CERT function (Computer Emergency Response Team)?   |           |  |  |
|                      |                                | IS.49 | Do you publish a roles and responsibilities document specifying what you vs. your customers are responsible for during security incidents?  |           |  |  |

|  |                                     |       |  |           |  |  |
|--|-------------------------------------|-------|--|-----------|--|--|
|  | Incident Reporting                  | IS.50 | Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting? |           |  |  |
|  |                                     | IS.51 | Does your logging and monitoring framework allow isolation of an incident to specific customers?   |           |  |  |
|  | Incident Response Legal Preparation | IS.52 | *Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?  | Mandatory |  |  |
|  |                                     | IS.53 | *Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?  | Mandatory |  |  |
|  |                                     | IS.54 | *Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific customer without freezing other customer data?                             | Mandatory |  |  |
|  |                                     | IS.55 | Do you enforce and attest to customer data separation when producing data in response to legal subpoenas?  |           |  |  |
|  | Incident Response Metrics           | IS.56 | Do you monitor and quantify the types, volumes, and impacts on all information security incidents?   |           |  |  |
|  |                                     | IS.57 | Will you share statistical information security incident   |           |  |  |

|                      |                         |       |   |           |  |  |
|----------------------|-------------------------|-------|---|-----------|--|--|
|                      |                         |       | data with your customers upon request?  |           |  |  |
|                      | Acceptable Use          | IS.58 | Do you provide documentation regarding how you may utilize or access customer data and/or metadata?   |           |  |  |
|                      |                         | IS.59 | Do you collect or create metadata about customer data usage through the use of inspection technologies (search engines, etc.)?  |           |  |  |
|                      |                         | IS.60 | Do you allow customers to opt-out of having their data/metadata accessed via inspection technologies?   |           |  |  |
| INFORMATION SECURITY | Asset Returns           | IS.61 | *Are systems in place to monitor for privacy breaches and notify customers expeditiously if a privacy event may have impacted their data?   | Mandatory |  |  |
|                      |                         | IS.62 | *Is your Privacy Policy aligned with industry standards and Indian Law  | Mandatory |  |  |
|                      | e-Commerce Transactions | IS.63 | Do you provide standard encryption methodologies (3DES, AES, etc.) to customers in order for them to protect their data if it is required to traverse public networks? (ex. the Internet) |           |  |  |
|                      |                         | IS.64 | *Do you utilize standard encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-                           | Mandatory |  |  |

|  |   |       |  |           |  |  |
|--|---|-------|--|-----------|--|--|
|  |   |       | based replication of data from one environment to another)?  |           |  |  |
|  | Audit Tools Access                      | IS.65 | Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.) |           |  |  |
|  | Diagnostic / Configuration Ports Access | IS.66 | *Do you ensure hardening of admin workstations and Role Based Access Control to enforce the 'least privilege' principle  | Mandatory |  |  |
|  | Network / Infrastructure Services       | IS.67 | Do you collect capacity and utilization data for all relevant components of your service offering?   |           |  |  |
|  |   | IS.68 | Do you provide customers with capacity planning and utilization reports?   |           |  |  |
|  | Portable / Mobile Devices               | IS.69 | *Do you allow mobile devices in your facility for administration purposes (e.g., tablets,)?  | Mandatory |  |  |
|  | Source Code Access Restriction          | IS.70 | *Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?          | Mandatory |  |  |
|  |   | IS.71 | *Are controls in place to prevent unauthorized access to customer application, program or object source code, and  | Mandatory |  |  |



|                       |                           |       |   |           |  |  |
|-----------------------|---------------------------|-------|---|-----------|--|--|
|                       |                           |       | assure it is restricted to authorized personnel only?   |           |  |  |
|                       | ESV Programs Access       | IS.72 | *Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?   | Mandatory |  |  |
|                       |                           | IS.73 | Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?   |           |  |  |
|                       |                           | IS.74 | *Are attacks which target the virtual infrastructure prevented with technical controls?   | Mandatory |  |  |
| LEGAL                 | Non-disclosure Agreements | LG.01 | *Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals? | Mandatory |  |  |
|                       | Third Party Agreements    | LG.02 | *Can you provide a list of current 3rd party organization that will have access to the customer's (My) data?  | Mandatory |  |  |
| OPERATIONS MANAGEMENT | Policy                    | OM.01 | Are policies and procedures established and made available for all personnel to adequately support services operations roles?   |           |  |  |
|                       | Documentation             | OM.02 | Are Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized  |           |  |  |

|  |                                       |       |  |           |  |  |
|--|---------------------------------------|-------|--|-----------|--|--|
|  |                                       |       | personnel to ensure Configuring, installing, and operating the information system?   |           |  |  |
|  | Capacity / Resource Resource Planning | OM.03 | Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?                     |           |  |  |
|  |                                       | OM.04 | *Do you restrict use of the memory oversubscription capabilities present in the hypervisor?  | Mandatory |  |  |
|  | Equipment Maintenance                 | OM.05 | If using virtual infrastructure, does your solution include hardware independent restore and recovery capabilities including offsite storage of backups?                                     |           |  |  |
|  |                                       | OM.06 | *If using virtual infrastructure, do you provide customers with a capability to restore a Virtual Machine to a previous state in time?   | Mandatory |  |  |
|  |                                       | OM.07 | *If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new provider?   | Mandatory |  |  |
|  |                                       | OM.08 | *If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location? | Mandatory |  |  |

|                 |                         |       |  |           |  |  |
|-----------------|-------------------------|-------|--|-----------|--|--|
|                 |                         | OM.09 | Do you share reports on your backup/recovery exercise results?   |           |  |  |
|                 |                         | OM.10 | Does your solution include software / provider independent restore and recovery capabilities?  |           |  |  |
| RISK MANAGEMENT | Program                 | RM.01 | Is your organization insured by a 3rd party for losses?  |           |  |  |
|                 |                         | RM.02 | *Do your organization's service level agreements provide customer remuneration for losses they may incur due to outages or losses experienced within your infrastructure?  | Mandatory |  |  |
|                 | Assessments             | RM.03 | *Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods? | Mandatory |  |  |
|                 |                         | RM.04 | Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?                       |           |  |  |
|                 | Mitigation / Acceptance | RM.05 | *Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?  | Mandatory |  |  |

|                      |                                  |       |   |           |  |  |
|----------------------|----------------------------------|-------|---|-----------|--|--|
|                      |                                  | RM.06 | *Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?   | Mandatory |  |  |
|                      | Business / Policy Change Impacts | RM.07 | *Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?  | Mandatory |  |  |
|                      | Third Party Access               | RM.08 | Do you monitor service continuity with upstream internet providers in the event of provider failure?  |           |  |  |
|                      |                                  | RM.09 | Do you have more than one provider for each service you depend on?  |           |  |  |
|                      |                                  | RM.10 | Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?  |           |  |  |
|                      |                                  | RM.11 | Do you provide the customer the ability to declare a disaster?  |           |  |  |
|                      |                                  | RM.12 | Do you provide a customer triggered failover option?  |           |  |  |
|                      |                                  | RM.13 | *Do you share your business continuity and redundancy plans with your customers?  | Mandatory |  |  |
| <b>SW DEPLOYMENT</b> | New Development / Acquisition    | SD.01 | *Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities? | Mandatory |  |  |

|                   |                                     |       |  |           |  |  |
|-------------------|-------------------------------------|-------|--|-----------|--|--|
|                   | Production Changes                  | SD.02 | *Do you provide customers with documentation which describes your production change management procedures and their roles/rights/responsibilities within it? | Mandatory |  |  |
|                   | Quality Testing                     | SD.03 | Do you provide your customers with documentation which describes your quality assurance process?   |           |  |  |
|                   | Outsourced Development              | SD.04 | *Do you have controls in place to ensure that standards of quality are being met for all software development?   | Mandatory |  |  |
|                   |                                     | SD.05 | *Do you have controls in place to detect source code security defects for any outsourced software development activities?                                    | Mandatory |  |  |
|                   | Unauthorized Software Installations | SD.06 | *Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?  | Mandatory |  |  |
| DISASTER RECOVERY | Impact Analysis                     | DR.01 | Do you provide customers with on-going visibility and reporting into your operational Service Level Agreement (SLA) performance?                             |           |  |  |
|                   |                                     | DR.02 | Do you provide customers with on-going visibility and reporting into your SLA performance?   |           |  |  |
|                   | Business Continuity                 | DR.03 | Are you BS25999 or ISO 22301 certified?  |           |  |  |

|              |                              |       |   |           |  |   |
|--------------|------------------------------|-------|---|-----------|--|---|
|              | y<br>Planning                |       |   |           |  |   |
|              |                              | DR.04 | Do you provide customers with geographically resilient hosting options?   |           |  |   |
|              | Business Continuity Testing  | DR.05 | *Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?   | Mandatory |  |   |
|              | Environmental Risks          |       | *Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?   | Mandatory |  |   |
|              | Equipment Power Failures     | DR.07 | *Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?  | Mandatory |  | □ |
|              | Power / Telecommunications   | DR.08 | Do you provide customers with documentation showing the transport route of their data between your systems?   |           |  |   |
|              |                              | DR.09 | Can customers define how their data is transported and through which legal jurisdiction?  |           |  |   |
| ARCHITECTURE | Customer Access Requirements | AR.01 | Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems? |           |  |   |

|  |  |       |  |           |  |  |
|--|--|-------|--|-----------|--|--|
|  |  | AR.02 | Do you use open standards to delegate authentication capabilities to your customers?   |           |  |  |
|  |  | AR.03 | *Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?  | Mandatory |  |  |
|  |  | AR.04 | Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access?   |           |  |  |
|  |  | AR.05 | Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a customer) if requested? |           |  |  |
|  |  | AR.06 | *Do you provide customers with strong (multifactor) authentication options (digital certs, tokens, biometric, etc...) for user access?   | Mandatory |  |  |
|  |  | AR.07 | Do you allow customers to use third party identity assurance services?   |           |  |  |
|  |  | AR.08 | Do you utilize an automated source-code analysis tool to detect code security defects prior to production?   |           |  |  |
|  |  | AR.09 | *Do you verify that all of your software suppliers adhere to industry standards for  | Mandatory |  |  |

|              |   |       |  |           |  |  |
|--------------|---|-------|--|-----------|--|--|
|              |   |       | Systems/Software Development Lifecycle (SDLC) security?  |           |  |  |
|              | Data Integrity                          | AR.10 | *Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data? | Mandatory |  |  |
|              | Production / Nonproduction Environments | AR.11 | *Do you provide customers with separate environments for production and test processes?  | Mandatory |  |  |
|              |   | AR.12 | Do you provide customers with guidance on how to create suitable production and test environments?   |           |  |  |
|              | Remote User Multifactor Authentication  | AR.13 | *Is multi-factor authentication required for all remote user access?   | Mandatory |  |  |
| ARCHITECTURE | Network Security                        | AR.14 | Do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?   |           |  |  |
|              | Wireless Security                       | AR.15 | *Are policies and procedures established and mechanisms implemented to protect network environment perimeter and configured to restrict unauthorized traffic?  | Mandatory |  |  |



|  |                          |       |   |           |  |  |
|--|--------------------------|-------|---|-----------|--|--|
|  |                          | AR.16 | *Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)  | Mandatory |  |  |
|  |                          | AR.17 | *Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?   | Mandatory |  |  |
|  | Shared Networks          | AR.18 | *Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations? | Mandatory |  |  |
|  | Clock Synchronization    | AR.19 | *Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?  | Mandatory |  |  |
|  | Equipment Identification | AR.20 | Is automated equipment identification used as a method of connection authentication to validate connection authentication   |           |  |  |

|  |                                     |       |   |           |  |  |
|--|-------------------------------------|-------|---|-----------|--|--|
|  |                                     |       | integrity based on known equipment location?  |           |  |  |
|  | Audit Logging / Intrusion Detection | AR.21 | *Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?                             | Mandatory |  |  |
|  |                                     | AR.22 | *Is Physical and logical user access to audit logs restricted to authorized personnel?  | Mandatory |  |  |
|  |                                     | AR.23 | *Can you provide evidence that due diligence mapping of currently applicable regulations and standards to your controls/architecture/processes has been done?   | Mandatory |  |  |
|  | Mobile Code                         | AR.24 | *Is mobile code tested (in terms of security) before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy? | Mandatory |  |  |
|  |                                     | AR.25 | *Is all unauthorized mobile code prevented from executing?  | Mandatory |  |  |