Request for Proposal for

Procurement, Provisioning, Validation and Management of Secured Infrastructure for KSFE's Software.

RFP NO: IT/14061/20/01

DATED 06 MAY 2020

The Kerala State Financial Enterprises Limited,

Bhadratha, Museum Road,
Thrissur -680 020.

Tel: 0487- 2332255

Email: etenders@ksfe.com

Table of Contents

Tender Document Details

Tender Ref No and Date	IT/14061/20/1 dt 06/05/2020
Last Date for seeking clarifications	17:00 hrs on 18/05/2020
Uploading of reply to queries	25/05/2020
Last date for submitting bid documents	17:00 hrs on 05/06/2020
Date of Opening Bids	11:00 hrs on 08/06/2020
Earnest Money Deposit/Bid Security	INR 5,00,000/-
RFP Cost	INR 29,500/-

Issued by:

The Managing Director,

Kerala State Financial Enterprises Limited,

Bhadratha, Museum Road,

Thrissur -680 020.

To,

All eligible vendors

KSFE invites sealed bids from Bidders to bid for Procurement, Provisioning, Validation and Management of secure Infrastructure for KSFE's various Software Platforms. (SMARTCustomer Web Portal, Mobile Application and Door Collection Agent's Mobile Application for ICT driven marketing)

Dear Sir / Madam,

Sub: **Procurement, Provisioning, Validation and Management of Secure Infrastructure for KSFE's various Softwares. (SMARTCustomer Web Portal, Mobile Application and Door Collection Agent's Mobile Application for ICT driven marketing)**

We request you to submit your proposal for Procurement, Provisioning, Validation and Management of secure Infrastructure for KSFE's Software which is scheduled to be live soon as per the technical specifications detailed in respective User Requirement Documents.

1. Procedure for Submission of Bids

Bidders are required to submit their bids in two-part bids (along with EMD and RFP Cost) consisting of the following, through this E-Tender. Interested bidders can submit their Technical bid and Commercial bids through the e tender site https://etenders.kerala.gov.in

Technical Bid (Part –I)

This should contain all technical details, Literature, Leaflets etc. confirmation of Commercial terms and conditions of the tender.

Commercial Bids (Part–II)

This should contain Prices against the bill of Quantity.

First Technical bid document of bidders will be evaluated and those who qualify this stage will be eligible for further evaluation. Commercial bids of only those bidders, who qualify the technical criterion, will be opened and evaluated further. The bidder has to remit the tender fee, EMD, Technical & Commercial bid through the e-tender website online.

EMD of the successful bidder will be returned only after successful execution of job against the Outline agreement /Purchase Order and submission of Performance Bank Guarantee. EMD of the unsuccessful bidders shall be returned after finalization of the successful Bidder.

KSFE does not take any responsibility for any delay in submission of online bid due to connectivity problem or non-availability of site. No claims on this account shall be entertained. Incomplete tenders shall be liable for rejection without seeking any further clarification. KSFE also reserve the right to reject any or all tenders without assigning any reasons whatsoever.

Every Tender should be accompanied by an agreement in the prescribed form (Annexure- 1) of Store Purchase manual on Kerala Government stamp paper worth Rs.200/- Any additional stamp duty legal charges etc. in respect of agreement will be borne by the bidder.(copy of agreement shall be attached with the Technical bid).

Every Tender should also be accompanied by a non-Disclosure Agreement in the prescribed form (Appendix – III) on Kerala Government stamp paper worth Rs.200/- Any additional stamp duty legal charges etc. in respect of agreement will be borne by the bidder (copy of agreement shall be attached with the Technical bid).

The bidder should submit hard copies of all the documents in triplicate other than the commercial bid submitted through the e-tender website to KSFE within 3 days after the last date of submitting the tender.

1.1 Pre Bid Queries

In case the bidder has any queries regarding the tenders, they should forward the queries to the email id etenders@ksfe.com on or before 17:00 hrs on 18.05.2020. No further queries/clarifications on this tender would be entertained after this date. Reply to the queries will be published in the e-tendering site. (Due to the existing conditions arisen out of COVID-19 and restrictions imposed by Government there won't be any pre-bid meeting and hence the above said query clarification procedure).

1.2 Contents of the Commercial Bid

Format of Commercial Bid is given in Proforma-1. The bidder shall quote the price of cloud services for 60 months, Cost of Deployment of proposed application in the cloud platform, and the charges for Operation and Maintenance of cloud environment for 60months. **Duly filled BOQ files should be uploaded in the e tender website.**

1.3 Contents of the Technical Bid

The Technical Bid consists of the following:

a) 5 Client references for successful completion / Purchase order for implementing cloud based digital experience.

b) Letter of Empanelment issued by MeitY, Govt. of India.

c) All relevant documents to substantiate bidder's eligibility criteria mentioned in this RFP.

1.4 Period of validity of Bids

Bids shall remain valid for 180 days from the date of opening of commercial bid prescribed by KSFE. A bid valid for a shorter period may be rejected by KSFE as disqualified.

In exceptional circumstances, KSFE may solicit the bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing, (or by fax/e-mail). The bid security validity shall also be suitably extended. A bidder may refuse the request without forfeiting his bid security. A bidder granting the request will not be required nor permitted to modify his bid.

1.5 General Instructions to Bidders for E-Tendering

Interested bidders may submit the tender in the CPP portal (http://etenders.kerala.gov.in) and participate in the tender as per the instructions given therein, on or before the due date of the tender.

Corrigendum / amendment, if any, shall be notified on the site http://etenders.kerala.gov.in Bidders are required to complete the following process online on or before the due date/time of closing of the tender:

1. Technical Bid
2. Commercial bid

Directions for submitting online offers, electronically, against e-procurement tenders directly through internet:

The system time (IST) that will be displayed on e-Procurement web page shall be the time considered for determining the expiry of due date and time of the tender and no other time shall be taken into cognizance. Bidders are advised in their own interest to ensure that their bids are submitted in e-Procurement system **well before the closing date and time** of bid. The bidder should ensure that **EMD submission through e-tender has been completed successfully**.

- Bids/Offers shall not be permitted in e-procurement system after the due date/ time of tender. Hence, no bid can be submitted after the due date and time of submission has elapsed.
- No manual bids/offers along with electronic bids/offers shall be permitted.
- No responsibility will be taken by KSFE and/or the e-procurement service provider for any delay due to connectivity and availability of website. They shall not have any liability to bidders for any interruption or delay in access to the site irrespective of the cause.
- KSFE and/or the e-procurement service provider shall not be responsible for any direct or indirect loss or damages and or consequential damages, arising out of the bidding process including but not limited to systems problems, inability to use the system, loss of electronic information etc.
- For any clarification pertaining to this tender, the bidder may use the email id etenders@ksfe.com

1.6 Right to accept or reject any or all bids

1) KSFE reserves the right to accept or reject any bids and to annul the bidding process and reject all bids at any time prior to award of the contract, without thereby incurring any liability to the affected Bidder or any obligation to inform the affected Bidder of the grounds for its action.

2) The acceptance of tender will rest with the KSFE, which does not bind itself to accept the best bid and reserves itself the right to reject any or all the tenders received without the assignment of any reason. All the bids in which any of the prescribed conditions are not fulfilled or are incomplete in any respect are liable to be rejected.

   The successful contractor will be required to furnish a Security Deposit in the form of a Bank Guarantee for an amount equal to 10% of the quoted value of the total cost for a period of 60 months with a claim period of further 3

months (i.e. 63 months from the date of commencement of contract). In the event of the contract being extended, the contractor will have to submit fresh bank guarantee covering the extended contract period as increased further by a period of 3 months for lodging the claim.

The successful contractor will be required to sign a Service Level Agreement with KSFE within 7 days from the date of purchase order.

2.0 Evaluation and Comparison of Bids

The objective of the evaluation process is to select a reliable and experienced Bidder(s), capable of installing a proposed solution which best meets the identified requirements, all within a reasonable time-frame at the lowest possible cost. In addition, the bidder must be willing and capable of providing ongoing maintenance that is responsive to the needs of KSFE in sustaining normal business operations. The bids will be technically evaluated as per the criteria specified in Minimum Eligibility Conditions and also on the basis of System functionality and design. The evaluation may include system demonstrations of cloud deployment and reference calls. The bidder offering the desirable solution with the best price will be selected. KSFE reserves the right to reject any or all proposals without assigning any reasons.

2.1 Verification

KSFE reserves the right to conduct a verification of the customer references submitted by the bidder. KSFE also reserves the right to conduct a verification of the quality management system in place, the manufacturing facilities, and the support infrastructure of the bidder. KSFE will conduct all or any of these verifications to satisfy itself on the bidder's capability to supply the tendered goods and services compliant to the requirement specifications defined in this tender. In the event of the verification revealing that a bidder does not have the capability to supply the

tendered goods and services compliant to the requirement specifications defined in this tender, KSFE may at its discretion reject the bid.

2.3 Award criteria

KSFE will review the Technical bids of the bidders to determine whether the Technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at KSFE's discretion. Subject to above, KSFE will award the contract to the successful Bidder whose bid has been determined to be substantially responsive and has been determined as the best-in Commercial bids, provided further that the Bidder is determined to be qualified to perform the contract satisfactorily.

The final contract will stipulate that the solutions specified will satisfy the Service requirements as stated in the RFP. The following documents would be included as attachments to the final contract:

- This Request for Proposal
- The bidder's proposal in response and clarifications made in course of the evaluation.
- An Implementation Plan identifying the tasks to be completed, the assigned responsibilities, and the scheduled completion dates.

2.4 Applicable Law

The Contract shall be interpreted in accordance with the laws of the Union of India & will be under the jurisdiction of courts at Thrissur.

2.5 Completeness of Response

a) Bidders are advised to study this RFP document carefully before submitting their

proposals in response to this RFP. Submission of a proposal in response to this RFP shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.

b) A bid shall be considered responsive only when the bidder's response to this RFP is full and complete in all respects including the compliance sheet.

c) Failure to furnish all the information required in this RFP or submission of a proposal not responsive to the RFP in all aspects will be at the Bidder's risk and may result in rejection of the bidder's Proposal.

2.6 Modification and Withdrawal of Proposal

No proposal may be withdrawn in between the deadline for submission of proposals and the expiration of the validity period specified by the bidder on the proposal form. Entire EMD may be forfeited if any of the bidders withdraw their bid during the validity period.

2.7 Non-Conforming Proposals

A proposal may be construed as a non-conforming proposal and ineligible for consideration if it does not comply with the requirements of this RFP. Failure to comply with the technical requirements, and non-acknowledgment of receipt of amendments, are common causes for holding proposals non-conforming.

2.8 Right to Modify Submission Deadline

KSFE may, at its discretion, extend the deadline for submission of proposals by issuing a corrigendum, in which case all rights and obligations of this RFP and the bidders previously subject to the original deadline will thereafter be subject to the deadline as extended.

2.9 Right to Terminate the Process

KSFE may terminate the RFP process at any time and without assigning any reason. KSFE makes no commitments, express or implied, that this process will result in a business transaction with anyone.

This RFP does not constitute an offer by KSFE. The bidder's participation in this process may result in KSFE selecting the bidder to engage in further discussions and negotiations toward execution of agreement. The commencement of such negotiations does not, however, signify a commitment by KSFE to execute agreement or to continue negotiations. KSFE may terminate negotiations at any time without assigning any reason.

2.10 Disqualification

The bid is liable to be disqualified in the following cases or in case bidder fails to meet the bidding requirements as indicated in this RFP:

- Proposal not submitted in accordance with the procedure and format prescribed in this document or treated as non-conforming proposal.
- The bidder qualifies the bid with his own conditions
- Bid is received in incomplete form
- Bid is not accompanied by all the requisite documents/EMD/RFP Cost.
- Information submitted in technical bid is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the Agreement (no matter at what stage) or during the tenure of the agreement including the extension period if any
- Commercial proposal is uploaded as part of technical proposal.
- Bidder tries to influence the proposal evaluation process by unlawful/corrupt/fraudulent means at any point of time during the bid process.

2.11 Payment Terms

KSFE will make payment subject to signing of the contract as follows: The Contract is initially for a period of 5 year. KSFE reserves the right to extend (after the expiry of the original contract) the period of the contract further for any period not exceeding 3 months at a time or till the next tender is finalized. The terms and conditions for the extended period will be same as that for the existing. The selected bidder/s have to claim the recurring charges quarterly in arrears on the achievement of SLAs. Any penalty arising out of non-compliance with SLA terms in a quarter would be adjusted in the charges for the ensuing quarter. The selected bidder/s should submit the uptime achieved to enable KSFE to pay the quarterly charges. All bills/invoices should be submitted to KSFE Head Office and payment will be released from KSFE Head Office.

3. Background

The Kerala State Financial Enterprises Limited, popularly known as **KSFE** came into existence in 1969, as a Miscellaneous Non-Banking Company (MNBC) owned by the Government of Kerala, started with the objective of providing an alternative to the private chit promoters with a view to socialize the chit fund business. The Company which started in a humble manner has now grown into an institution doing business worth over Rs.40,000 crores annually, employing over 7000 persons directly and over 5000 persons indirectly, with a network of over 575 branches. The main activities of this organisation are Chitties, Sugama, Loans and Fixed Deposits. KSFE has set a business target of 100Lakhs subscriber base and a turnover of 1 lakh crore by 2022.

KSFE is in the process of developing a new software/s to provide online enrollment, remittances to its various schemes. KSFE envisages to achieve its 2022 targets mainly through such new digital channels. This RFP for a secured and highly scalable infrastructure is invited for deploying newly developed apps in line with the above objective.

Scope of Work: Description of Services for Managed Services Provider

A. One-time Integration Services for : Provisioning and Validation of Secure Infrastructure

A.1 Establishing (or adapting any existing) CSP accounts

- Establishing the security and compliance framework and creating the security control design as agreed

A.2 Network Infrastructure Design and Provisioning

- IAM based roles and policies for CSP services
- Complete infrastructure configuration for virtual networks.
- Configure subnets, security group rules, network access control list, route table rules
- Configure connectivity for inbound and outbound access

A.3 Application Infrastructure provisioning

- Provision production, dev and QA instance according to specifications
- Provision AI instance
- Provision Database server
- Configure security for all provisioned servers

A.4 Support Application Setup, Testing and Production Deployment

- Provide infrastructure troubleshooting assistance during functional testing
- Support production deployment of applications and go-live activities

B. Ongoing Infrastructure Managed Services (For the period of Contract)

B1 Remote Infrastructure Monitoring

- Daily remote monitoring of all production, development and QA instances in-scope
- Monitor storage/space issues and manage any capacity issues
- Configure and manage alarm notification list

- Set-up and configure CSP audit trail, application and infrastructure monitoring
- Configure connectivity for inbound and outbound access
- Support Customer in creation and management of DNS records
- Manage existing routing tables, subnets/or edit existing subnets
- Management of IP Ranges and static IP allocation management
- Gateway Management (CSP to CSP or CSP to on premise)
- Management of Security Groups (Creation / Editing / Management)

B2 Backup and Restore

- Determine / adhere to the appropriate local and/or offsite backup requirement as well as data retention policy

B3 Patching

- Update and patch all systems in a timely and secure manner including (OS updates/upgrades; resizing storage volumes for growth).
- Implement patches as early as practical after the release
- Patches should be applied with minimal disruption to production operations
- Test and apply non-critical vendor software patches according to an agreed upon schedule
- Perform regular maintenance of the environment, addressing event log errors and warnings

B4 Incident Management

- Monitors the overall health of your infrastructure resources, and handles the daily activities of investigating and resolving incidents.
- Propose Incident/Problem workflow, escalation, communication and reporting processes that support the Service Level Requirements
- Troubleshoot and triage tickets using available tools and knowledge bases
- Manage entire Incident/Problem resolution lifecycle, including detection, diagnosis, progress reporting, repair and recovery, documentation and knowledge base updates
- Record resolution in the ticketing system
- Ensure Incident Resolution activities conform to defined Change Control procedures

- Track and report monthly recurring Incidents, problems and failures and communicate associated consequences to Customer.
- Recommend solutions to Customer to address trends, recurring Incidents, problems or failures
- Review and approve solutions to address trends, recurring incidents, problems or failures
- Notify stakeholders of the incident with an ETA for resolution

B5 Security and Access Management

- Protect information assets and keep CSP infrastructure secure.
- Setup anti-malware protection, intrusion detection, and intrusion prevention systems
- Manage security policies and quickly respond to any intrusion
- Configure CSP security capabilities and best practices, such as Identity and Access Management (IAM) roles and virtual firewall security

B6 Cost Management

- Provide a monthly summary of key performance metrics, including operational activities, events and their respective impact, as well as recommendations to optimize platform usage and optimize cost so as to get the most out of CSP investment.

B7 Knowledge Management

- Document procedures manual, run book, operations and administration procedures that meet requirements and adhere to defined policies
- Document operations and administration procedures

B8 Operational reporting

Provide monthly status reviews including reporting depicting performance against each service level requirement as below

- Utilization report (Resource usage report)
- Incident / Change reports
- Ticketing reports
- Cost reports
- Security reports (logins, intrusion, denial of service (DDOS), and other anomalies)Provide periodic status reviews to the stakeholders to discuss incident activity, enhancement work (including backlog and new requests), planning and issue resolution

C. Express Connectivity between Cloud Service Active Zone and IDC Ahmedabad

- Assured 24/7 full redundancy express connectivity between cloud active zone and IDC Ahmedabad.

4. ELIGIBILITY CRITERIA OF THE BIDDERS

KSFE will use the following as the Minimum Eligibility Criteria (MEC) for this RFP and evaluating bidders. The bidder fulfilling the following criteria only should respond to the RFP/Tender:

ELIGIBILITY CRITERIA

Sl. No.	Technical Parameters	Support Documents to be submitted	Compliance (File name, Page no.)
	Eligibility Criteria for Managed Service Provider (MSP)		
1	The sole Bidder or Lead member in the case of Consortium, as a single legal entity, must be registered in India and should have been in operations in India for a minimum of three (3) years by the date of opening of the bid.	Certificates of incorporation / Registration Certificates along with Bylaws/ MoA & AoA or similar legal document.	

2	Bidder must submit a clause-by-clause compliance certificate establishing the conformity of the technical specification as mentioned in Section 2 by clearly indicating 'complied' or 'not complied' along with cross reference from the proposed CSP. A bid without clause-by-clause compliance of the Technical Specifications shall not be considered.	Compliance certificate	
3	The sole bidder or lead member in the case of consortium must be registered under appropriate authorities i.e. must be registered with GST authorities/PAN etc.	Copy of GST / PAN	
4	The sole bidder or lead member or any member of its consortium in the case of consortium must have minimum cumulative turnover of 5 Crores cumulatively in the last three (3) Financial Years (2016-2017, 2017-18, 2018-19).	Audited financial statements for last three Financial Years along with CA certificate clearly specifying turnover.	
5	As on date of submission of the proposal, the sole bidder or Lead member or any member of its consortium shall not be blacklisted by any Central Government Department in Government of India/ State Government Departments of any state/ PSU entities in the last 3 years.	Letter of undertaking to this effect on the letter head, signed by bidder's authorized signatory.	
6	The sole bidder or the lead member or any member of its consortium should be a Cloud Services Provider or an authorized partner of the proposed Cloud Service Provider.	Authorization letter issued by the Cloud Service Provider specific to this RFP	

7	The sole bidder or the lead member or any member of its consortium should have experience of implementing minimum 5 cloud based digital experience, single view of customer, cross-channel customer experience and messaging platforms in India out of which at least two should be for State / Central Government / PSU entities	Copy of purchase order/completion certificate indicating the nature of work should be submitted. The bidder should submit details like name of contact person along with his phone number for above projects to be submitted for verification.	
	Eligibility Criteria for Cloud Service Provider (CSP)		
8	Bidder must propose CSP, which is audited, by STQC and MeitY empaneled.	Letter of Empanelment issued by MeitY, Govt. of India.	
9	Cloud Service Provider should feature in the Leaders Quadrant of Gartner's Magic Quadrant for Infrastructure as a Service (IaaS) offering of Public Cloud – 2018 Report or later.	Valid Proof for Existence in Gartner's Magic Quadrant shall be produced	
10	Cloud Service Provider should have the following third-party certifications: a. ISO 9001 - International Standard for Quality Management Systems b. ISO 27001 - Information Security Standard c. ISO 27017 - Security Controls for Cloud Services d. ISO 27018 - Standard for the Protection of Personal Data in Cloud	Copy of Valid Certificates	
11	Cloud Service Provider should have the following additional accreditations: a. SOC1 b. SOC2 c. SOC3 d. PCI-DSS 3.2 Level 1	Self-Certificates issued by the Cloud Service Provider.	

12	Availability SLA on the compute and block storage services offered by the CSP in India should be >= 99.99%	Proof of Published SLAs in the Public Portal of the Cloud Service Provider.	
13	Cloud Service Provider should have Self-Service software defined configurations to add / remove capacity. Customer should have full control on the environment e.g., can create a virtual private cloud, create or stop a VM, add or remove storage, create a database instance, configure security parameters, etc and also has the ability to log, monitor, and audit the traffic and usage	Demonstration on the Cloud Service Provider's online console	

Technical Evaluation Criteria

Sl. No.	Technical Parameters	Maximum Score	Marks Distribution	Bidders Response
1	Lead bidder or consortium partner /Cloud service provider Project Experience: Cloud based cross-channel customer experience and messaging platforms in India	20	Greater than 25 Projects: **20 marks** Between 10 – 25 Projects: **10 marks** Between 5-10 Projects: **5 marks** Less than 5 Projects: **0 marks**	
2.	Unique Value Proposition of the offered Solution and Quality of Service offered by the CSP in India.	40	I. The proposed solution is required to be a multi-site deployment, across geographically disparate sites, with Active-Active configuration to ensure fault-tolerance with high availability between two physical sites. In case of failure, automated processes to shift application traffic to a secondary physical site: **10 marks** II. Proposed solution with incremental block	

			SSD storage with minimum increments of 10 GB or below so that department pays exactly for actual usage: **10 marks** III. Proposed Solution offering geo-redundant object storage to ensure redundancy and high durability of the data: **10 marks** IV. CSP capability to provide dedicated server/host using its native Cloud Infrastructure (hardware) in India, which allows usage of existing software license to deploy: **5 marks** V. Availability SLA of >= 99.99% on the compute and block storage services offered by the CSP as per the published SLAs of the CSP: **5 marks**	
3	Platform Services	20	Availability of relevant native PaaS services from the CSP for the current requirement**:** I. Cloud Service Providers must offer a Digital Engagement as a PaaS Service that enables effective communication with end users and measure user engagement across multiple channels including email, Text Messaging (SMS) and Mobile Push Notifications: **8 marks** **II.** Relational Database as a Services for all Major RDBMS (Oracle, MSSQL, MySQL, PostgreSQL)**: 8 marks** III. Data warehousing / Data Lake: **2 marks** **IV.** Machine learning / Artificial Intelligence: **2 marks**	
4	Technical Presentation and Demonstration	20	A. Technical Presentation: **5 marks** B. Demonstration on the CSP's online console: **15 marks** Agility – Self-Service software defined configurations to add / remove capacity. Customer has the full control on the environment (e.g., can create a virtual private cloud) and has the ability to log, monitor, and audit the traffic and usage	

Note:

1. Bidders, whose bids are responsive, based on minimum qualification criteria / documents as in Pre- Qualification Criteria and score at least 80 in the Technical Evaluation Criteria would be considered technically qualified. Commercial Bids of such technically qualified Bidders alone shall further be opened.
2. Schedule for technical presentation will be communicated to bidders who qualify Pre-Qualification criteria. It is mandatory for bidders who qualify Pre-Qualification criteria to appear for Technical Evaluation Presentation else the bid would not be considered for further evaluation. Proposer need to submit the soft copy and hard copy of the technical presentation at the time of technical presentation.

Evaluation and Comparison of Bids

The objective of the evaluation process is to select a reliable and experienced Bidder(S), capable of setting up the Cloud Platform, which best meets the identified requirements, all within a reasonable time-frame at the best possible cost. The bids will be technically evaluated as per the criteria specified in Technical Bid evaluation criteria given in the table. The bidder offering the desirable solution with the best price will be selected. KSFE reserves the right to reject any or all proposals.

Total Score

The method of selection is Quality cum Cost Based Selection (QCBS) using 60 and 40 weightage quality (Technical bid score) and cost respectively.
The following equation would be used to calculate the total score of the bidders based on the technical bid score and commercial bid.

$B= (C_{low}/C)X + T/T_{high}(1-X)$
C_{low} = the lowest of all the bids among the responsive bids
T_{high} = The technical score achieved by the bid that was scored best among all the responsive bids.
C = Evaluated bid price
T = Technical score awarded to the bid
X = Weightage for the cost.

Technical Specifications of Proposed Cloud Services:

S.No	Description	CSP Offering with Cross Reference
1	**Compute Service:** a) Compute instances offered should be latest generation processor (intel Xeon Platinum processor or higher) b) Physical core to vCPU ratio should not more than 1:2 for the proposed VMs as well as for additional VMs required during contract period. c) Self-service provisioning of multiple VMs concurrently either through a programmatic interface or Web Portal d) Architected in such a way to automatically restart VMs on a healthy host if the original physical host fails and avoid VM outages or downtime when the provider is performing any kind of hardware or service maintenance at the host level e) Schedule events for VMs, such as a reboot, stop/start, or retirement f) Ability to automatically increase/scale the number of Instances/VMs during demand spikes to maintain performance g) Pause and Resume VMs (hibernate compute instances when not required and resume them from this state at a later time) h) Ability to place instances in multiple distinct locations / separate availability zones to protect applications from failure of a single location i) Capability to provide compute instances available as single tenant Instances/VMs that run on hardware dedicated to a single user. Capability should be available using CSPs native cloud Infrastructure in India region. j) Support for Operating Systems: Linux, RHEL, Suse Linux Enterprise, Windows. k) Uptime SLA of 99.99% in Proposed CSPs India region	

2	Block Storage a) Self-service provisioning of storage either through a programmatic interface or Web Portal b) Ability to increase the size of an existing block storage volume without having to provision a new volume and copy/move the data; c) Ability to dynamically increase capacity, tune performance, and change the type of live volumes with no downtime or performance impact. d) Ability to provision storage in minimum increments of 10 GB or below so that customer pays exactly for actual usage e) Supports point-in-time snapshots, that are incremental in nature to speed up provisioning and recovery f) Offers server-side encryption of data 'at-rest', i.e., data stored on volumes and snapshots g) Ability to provide a simple, automated way to back up data stored on volumes by ensuring that snapshots are created and deleted on a custom schedule. User should no longer need to use scripts or other tools to comply with data backup and retention policies. h) Ability to provide seamless encryption of data volumes, boot volumes and snapshots, eliminating the need to build and manage a secure key management infrastructure. i) Uptime SLA of 99.99% in Proposed CSPs India region. j) CSP Should offer choice of block storage: i. Provisioned IOPS: To deliver a consistent baseline performance of up to 50 IOPS/GB to a maximum of 64,000 IOPS and provide up to 1,000 MB/s of throughput per volume. ii. SSDs: To Deliver a consistent baseline performance of 3 IOPS/GB to a maximum of 16,000 IOPS, and provide up to 250 MB/s of throughput per volume. iii. Throughput Optimized HDD: To deliver performance in terms of throughput, measured in MB/s, and include the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume. iv. Cold HDD: To deliver up to 80 MB/s per TB, with a baseline throughput of 12 MB/s per TB and a maximum throughput of 250 MB/s per volume.	

3	**Object Storage** a) Self-service provisioning of storage either through a programmatic interface or Web Portal b) Proposed Solution offering geo-redundant object storage to ensure redundancy and high durability of the data c) Offer object storage tiering capability, i.e. the ability to recommend transitioning an object between object storage classes based on its frequency of access d) Support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation to deletion e) Ability to create and use policies to manage stored data, its lifecycle, and tiering settings f) Capability to create policies that can restrict access to the data based on user/request location and time of request g) Support hosting static websites out of its object storage service h) Support server-side encryption (SSE) of data 'at-rest', with the cloud provider managing the encryption keys or customer provided cryptographic keys i) Support read-after-write consistency for PUT operations for new objects j) Support versioning, i.e. the ability to store and co-exist multiple versions of an object k) Capability for a user to mark an item as undeletable l) Support multi-factor authentication (MFA) for delete operations as an additional security option m) Ability to send notifications when certain events happen at the object level (i.e. addition/deletion operations) n) Capability of generating audit logs that include details about a single access request, such as the requester, the request time, the request action, the response status, and the error code o) Provider allow uploading an object as a set of parts where each part is a contiguous portion of the object's data and these objects parts can be uploaded independently and in any order p) Object inventory to give user's ability to quickly visualize objects and their status, allowing users to quickly spot objects with public access q) Ability to route data (i.e. upload) from edge locations to the storage service using an optimized network path r) Users the ability to retrieve only a subset of data from an object by using simple SQL expressions s) Feature to block object version deletion during a customer-defined retention period so that you can enforce retention policies as an added layer of data protection or to meet compliance obligations t) Supports both server-side encryption (with three key management options) and client-side encryption for data uploads.	

4	**Network & Firewall** a) Capability to protect servers based on protocols and ports. b) Capability to protect network subnets with access controls that provides an optional layer of security that provides a stateless firewall for controlling traffic in and out of a subnet c) Capability to segregate public subnet and private subnet d) Capability to configure route tables that define which subnets are allowed to route external traffic over backend VPN or site-site connections, virtual network peering connections, Internet connections, or even specific virtual machine instances. e) Prevent packet sniffing: Virtual instances should be designed to p3revent other instances running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. Even if tenants configure interfaces into promiscuous mode, the hypervisor should not deliver any traffic to them that is not addressed to them. f) Prevent IP Spoofing: the cloud service should not permit an instance to send traffic with a source IP or MAC address other than its own.	
5	**Implement Identity and Access Management (IAM)** to properly separate users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks**.** Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the user account.	
6	**Multi-factor authentication (MFA)** to prove physical possession of a hardware or virtual MFA device for the root account, as well as any privileged Identity and Access Management accounts associated with it	
7	**DNS as Service:** Highly available and scalable cloud Domain Name System (DNS) web service with features like DNS Failover, DDOS Mitigation, Geo DNS, Latency Based Routing, Weighted Round Robin (WRR) functionality Private DNS for cloud-based servers, access to management console. The service should support internal domain names for intranet portals.	
8	**Web Application Firewall:** Protection from attacks by filtering traffic based on rules that you create. Filter web requests based on IP addresses, HTTP headers, HTTP body, or URI strings, which allows you to block common attack patterns, such as SQL injection or cross-site scripting that could affect application availability, compromise security, or consume excessive resources. Features like protection against Web Traffic visibility, east of deployment and maintenance, integrated security.	

9	**Distributed Denial of Service (DDoS) Protection:** Managed DDoS protection service that defends against most common, frequently occurring network and transport layer DDoS attacks that target web site or applications. When used with Content Delivery Network and global DNS service, should provide comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks. Should provide always-on detection and automatic inline mitigations, minimize application downtime and latency.	
10	**Managed Threat Detection Service**: Continuously monitor for malicious or unauthorized behavior to help you protect your accounts and workloads. It should monitor for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. The service should also detect potentially compromised instances or reconnaissance by attackers.	
11	**Monitoring** a) Monitoring Services for resources: Capability to monitor cloud environment centrally, custom monitoring metrics, monitor and store logs, view graphs & statistics, set alarms, monitor and react to resource changes. Support monitoring of custom metrics generated by your applications and services and any log files your applications generate. Gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly. b) Personal Health Dashboard: Provide alerts and remediation guidance when CSP is experiencing events that may impact the customer. Personalized view into the performance and availability of the Cloud services underlying your Cloud resources. **c)** Cloud Advisor: Capability to analyze your Cloud environment and provides best practice recommendations (or checks) in five categories: cost optimization, security, fault tolerance, performance, and service limits. Security checks should include monitoring of cloud resources on security configuration gaps, such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies.	

12	**Compliance** **a)** Audit: Capability to provide and record logs of all user activity within a cloud environment including actions taken through the CSP's Management Console, CSP's SDKs, command line tools, and other CSP services. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the Cloud service. The API activity history should be delivered within a reasonable timeframe (<30 minutes) from the time API call is made. Capability to support storing log files in a durable and inexpensive storage solution. **b)** Network logs: Capability to capture information about the IP traffic going to and from network interfaces in your virtual network that can be used to troubleshoot why specific traffic is not reaching an instance, or as a security tool to monitor the traffic that is reaching your instance. **c)** Governance and Compliance: Capability to discover all of cloud resources and view the configuration of each. Continuously monitor and record your Cloud resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. Receive notifications each time a configuration changes, as well as dig into the configuration history to perform incident analysis. Capability to obtain details of what a resource's configuration looked like at any point in the past. Capability to notify every configuration change so customers can process these notifications programmatically.	
13	**Certificate Authority:** Service to provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with could services. Service should enable creation of private certificates for customer's internal resources and manage the certificate lifecycle centrally. Service should also allow import of SSL/TLS certificates issued by third-party Certificate Authorities (CAs) and deploy them on cloud services such as load balancers and content delivery networks including monitoring the expiration date of an imported certificate, and importing a replacement when the existing certificate is nearing expiration.	
14	**Data Transfer:** a) One Time: Capability to migrate peta byte scale data from on premise to cloud. **b)** On-going: High speed dedicated network connectivity from on premise environment to cloud	

DATA RESIDENCY

The entire data shall be stored in systems located in India only. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction.

SLA Management

a. Service Levels will include Availability Measurements and Performance measurements
b. Availability and Performance report should be provided on monthly basis at the end of every month containing all the incidents reported to KSFE. The Bidder has to provision suitable tools to generate such reports. The reporting format to be finalized in consultation with KSFE.
c. The quarterly SLA reports should be provided by the Bidder to KSFE within seven days from the last date of each quarter.
d. The SLA reports shall be jointly reviewed by the Bidder and KSFE within next seven working days. In case of the service level deviations, penalty will be calculated as per Service Levels Agreement and charged to the Bidder
e. Bidder has to ensure support on 24x7x365 basis.
f. The Bidder will be a Single Point of Contact for KSFE and will be responsible to manage end to end SLA over the tenure of the contract.

Service Availability

General goal is to provide Service Availability Twenty Four hours per day, 7days per week except during times of Service Maintenance informed in advance to KSFE. All efforts shall be made to make the target Service Availability 99.99% network uptime except during scheduled service maintenance.

Support Availability

Cloud/Managed Service Provider shall have its own facilities to identify the incidents related to networks and remedial measures must be initiated on its own. All incidents reported by KSFE offices shall be recorded and validated and Incidents requiring support shall be handled in co-ordination with the respective OEMS.

Severity Level	Explanation	Ticket Response Goals	Ticket Resolution Time
Level – 1 Emergency	Production Cloud or the Cloud Dashboard is down, business operations severely impacted with no workaround; or a security issue.	Within 30 Minutes	Within 2 hours

Level – 2 High	Production Cloud or Cloud Dashboard is operational but significant disruption of business operations; no stable workaround.	Within 1 hour	Within 4 hours
Level – 3 Medium	Issues causing moderate to low business disruption with a Production or Development Cloud or the Cloud Dashboard or any issue for which there is a stable workaround available.	Within 2 hours	Within 24 hours
Level – 4 Low	Production or Development Cloud is operational, as is the Cloud Dashboard; no significant disruption of business operations; issues with little time sensitivity such as general questions	Within 4 hours	Within 72 hours

Financial Penalties for SLA Violations

In the event that Cloud fails to meet the guarantee stated above (excluding Service Maintenance and downtime caused by reasons described below), MSP will be charged 2% of the Customer quarterly service Fees for each thirty (30) minutes of network downtime experienced up to 100% of the quarterly service Fee for those Services affected.

For each quarter, if the Penalty amount goes greater than 50% of the total quarterly service value, then Second Party will consider the service as below par and may take further corrective actions including the Termination of the contract

Exclusions:

a) Any Service Maintenance that may cause Severity Level 1 errors must be limited to One hour per month.

b) The Service Availability goals exclude any time Customer requests a Cloud be taken down for scheduled updates.

c) Unavailability of service due to Force Majeure

4.1 Breakup of Cloud Services (Main)

S. No	Items (with minimum specifications)	CPU	OS Size - SSD (GB)	Memory Size (GB)	UoM	QTY (A)	Unit Price of VM - Committed Usage (B)	Price of SSD based OS Disk (C)	Price of Data Disk (D)	Price of Snapshots of VM & Data for backup (E)	Total Price Per Month F=A*(B+C+D+E)	Total Price for 5 Years (Excluding Taxes) (G=F*60)	Taxes (H)	Total Price inclusive Taxes (I=G+H)
	Virtual Machines **Bidder / CSP should ensure that physical core to vCPU ratio is not more than 1:2 for all proposed VMs**													
1	Production Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	4	200 + EBS	16	Per VM / Month	2								
2	Development Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	4	100 EBS only	16	Per VM / Month	3								
3	Production Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	20	150	100	Per VM / Month	1								
4	Production - DB Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	20	450	100	Per VM / Month	1								

5	Mongo DB Atlas (M50 - SaaS from MongoDB 3 node cluster)		160	32	GB/Year	1								

S. No	Items (with minimum specifications)	Description	UoM	QTY (A)	Unit Price (B)	Total Price Per Month C=A*B	Total Price for 5 Years (Excluding Taxes) (D=C*60)
1	Support Storage Volumes	General purpose SSD	200 GB	2			
2	Balancer			2			
3	Static Public IP			2			

	Items (with minimum specifications)	Description	UoM	QTY (A)	Unit Price (B)	Total Price Per Month C=A*B	Total Price for 5 Years (Excluding Taxes) (D=C*60)	Taxes (E)	Total Price inclusive Taxes (F=D+E)
	Network, Security, storage& Monitoring Services								

1	Load Balancer		Per VLB / Month	2					
2	DNS Service	Domain Naming System for routing traffic	Per DNS / Month	1					
3	Client VPN Connections	For providing secured connectivity per client to proposed cloud environment	Per Connection / Month	1					
4	Public IP	Dedicated Public IP	Per IP / Month	2					
5	Data Transfer (In) (onsite to Cloud)		Per GB / Month	100					
6	Data Transfer (Out) (onsite to Cloud)		Per GB / Month	100					
7	Web Application Firewall (Layer 7 Security)	Number of rules & request	Rules & Requests / Month	7					
8	Backup Storage	Backup storage in object store	Per GB / Month	500					
9	Archival Storage	Archival Storage for Long Retention (Above 90 Days)	Per GB / Month	500					
10	Resource Monitoring Dashboards	Visualize CPU, Memory, Disk utilization, Raise Alarms for Threshold breach	Per Month	1					

11	Virtual Firewall – VM Level & Subnet Level	Allow / Deny inbound & outbound traffic	Per Firewall / Month	1					
12	In memory based distributed caching service.								
13	Managed Queue service								
14	Container Orchestration with deployment tool for Prod								

Breakup of Cloud Services (Optional to be procured within 1 year. Network Bandwidth upto 10 Gbps)

S. No	Items (with minimum specifications)	CPU	OS Size - SSD (GB)	Memory Size (GB)	UoM	QTY (A)	Unit Price of VM - Committed Usage (B)	Price of SSD based OS Disk (C)	Price of Data Disk (D)	Price of Snapshots of VM & Data for backup (E)	Total Price Per Month F=A*(B+C+D+E)	Total Price for 5 Years (Excluding Taxes) (G=F*60)	Taxes (H)	Total Price inclusive Taxes (I=G+H)
	Virtual Machines **Bidder / CSP should ensure that physical core to vCPU ratio is not more than 1:2 for all proposed VMs**													
1	Production Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	4	50 + EBS	16	Per VM / Month	2								

2	Production Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	8	500	32	Per VM / Month	1								
3	Production Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	16	1500	32	Per VM / Month	1								
4	Production Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	16	1000	32	Per VM / Month	11								
5	Development Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	4	EBS	16	Per VM / Month	3								
6	Development Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	4	500	8	Per VM / Month	1								
7	Development Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	8	1500	16	Per VM / Month	2								
8	Production Linux/Unix, CentOS 7 / Ubuntu 18.04 LTS | 64-bit	2	100	16	Per VM / Month	1								

S. No	Items (with minimum specifications)	Description	UoM	QTY (A)	Unit Price (B)	Total Price Per Month C=A*B	Total Price for 5 Years (Excluding Taxes) (D=C*60)
1	Load Balancer			2			

1. UNPRICED BILL OF MATERIAL

Bidder to Submit the unpriced Bill of Material as part of Technical Bid in the below format. Please note that all the price items indicated in the financial bid format should be offered. Absence of any of the line item shall be considered as incomplete bid and shall lead to disqualification.

Sl.No.	Items (with minimum specifications)	Qty Offered	CSP Offering with Cross Reference to Public URL

2. COMMERCIAL BID:

Name, Address & Contact No. of the Company:

Commercial bid

S.No	Item Description	Qty	Basic Price	Taxes	Total Price
1	Installation of applications to proposed Cloud environment.	Lumpsum			
2	Cloud Services (as per breakup in section 4.1)	60 Months			
3	Operation & Maintenance of Cloud environment as per specified scope of work. Should include Exit Management.	60 Months			
4	Express connectivity between cloud activism and IDC	60 Months			
	GRAND TOTAL				

Annexure 1: Format of Agreement

Agreement

Articles of agreement executed on this the ….....…..day of ..... two thousand sixteen **BETWEEN** the Managing Director , KSFE Ltd., (hereinafter referred to as "KSFE") of the one part and Sri.....……..... .... ……. (H.E. name and address of the tender) (Here in after referred to as "the bounden") of the other part.

WHEREAS in response to the Notification No.....dated…..... the bounden has submitted to the Government a tender for the ..... the specified therein subject to the terms and conditions contained in the said tender;

WHEREAS the bounden has also deposited with the Government a sum of Rs.....…….....as earnest money for execution of an agreement undertaking the due fulfillment of the contract in case his tender is accepted by the Government.

NOW THESE PRESENTS WITNESS and it is hereby mutually agreed as follows:

In case the tender submitted by the bounden is accepted by the KSFE and the contract for ….....…… is awarded to the bounden, the bounden shall within …..... days of acceptance of this tender execute an agreement with the KSFE incorporating all the terms and conditions under which the KSFE accepts his tender.

In case the bounden fails to execute the agreement as aforesaid incorporating the terms and conditions governing the contract, the KSFE shall have power and authority to recover from the bounden any loss or damage caused to the KSFE by such breach as may be determined by the KSFE by appropriating the earnest money deposited by the bounden and if the earnest money is found to be inadequate the deficit amount may be recovered from the bounden and his properties movable and immovable in the manner hereinafter contained.

All sums found due to the KSFE under or by virtue of this agreement shall be recoverable from the bounden and his properties movable and immovable under the provisions of the Revenue Recovery Act for the time being in force as through such sums are arrears of land revenue and in such other manner as the KSFE may deem fit.

In witness whereof Sri.....……..... (Name and designation) for and on behalf of the KSFE and Sri..…….....the bounden have hereunto set their hands the day and year shown against respective signatures.

Signed by Sri.....……. (date).....

In the presence of witnesses:

1. .....……

2. .....……

Signed by Sri……..... (date).....

In the presence of witnesses:

1. .....……

2. ….....

Annexure 2 : Abbreviations

Acronym	Full Form
API	Application Program Interface
CA	Certificate Authority
CPU	Central Processing Unit
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
DNS	Domain Name System
GB	Gigabyte
HTTP	HyperText Transfer Protocol
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IOPS	Input/Output Operations Per Second
MeitY	Ministry of Electronics and Information
MFA	Multi Factor Authentication
MSP	Managed Service Provider
PCI-DSS	Payment Card Industry Data Security Standard
PSU	Public Sector Unit
RDBMS	Relational Database Management System
RHEL	Redhat Enterprise Linux
SDK	Software Development Kit
SLA	Service Level Agreement
SOC	Service Organization Control
SQL	Structured Query Language
SSL	Secure Socket Layer
STQC	Standardisation Testing and Quality Certification
TB	Terabytes

TLS	Transport Layer Security
UoM	Unit of Measure
URL	Uniform Resource Locator
vCPU	Virtual Central Processing Unit
VM	Virtual Machine
VPN	Virtual Private Network

Annexure - III

Non-Disclosure Agreement (NDA)

(On INR 200 stamp paper)

To, Date:

The Managing Director

KERALA STATE FINANCIAL ENTERPRISES LTD.,

"BHADRATHA",

Chembukavu, Thrissur-680 020

Confidentiality Undertaking

We acknowledge that during the course of tendering for Cloud services in Kerala State Financial Enterprises Ltd., we may have access to and be entrusted with Confidential Information. In this letter, the phrase "Confidential Information" shall mean information (whether of a commercial, technical, scientific, operational, administrative, financial, marketing, business, or intellectual property nature or otherwise), whether oral or written, relating to its business that is provided to us pursuant this Agreement. In consideration of you making Confidential Information available to us, we agree to the terms set out below:

1. We shall treat all Confidential Information as strictly private and confidential and take all steps necessary (including but not limited to those required by this Agreement) to preserve such confidentiality.
2. We shall use the Confidential Information solely for the preparation of our response to the RFP/Contract and not for any other purpose.
3. We shall not disclose any Confidential Information to any other person or firm, other than as permitted by item 5 below.
4. We shall not disclose or divulge any of the Confidential Information to any other clients or OEMs or third party.
5. This Agreement shall not prohibit disclosure of Confidential Information:
    - To our partners/directors and employees who need to know such Confidential Information to assist with the bidding for RFP floated for Cloud Services (Ref: RFP IT/14061/19/XX).
    - With your prior written consent, such consent not to be unreasonably withheld;
    - To the extent that such disclosure is required by law;
    - To the extent that such disclosure is required by any rule or requirement of any regulatory authority with which we are bound to comply; and
    - To our professional advisers for the purposes of our seeking advice. Such professional advisors will be informed of the need to keep the information confidential.
6. Upon your request we shall arrange delivery to you of all Confidential Information, and copies thereof, that is in documentary or other tangible form, except:
7. For the purpose of a disclosure permitted by item 5 above; and
8. To the extent that we reasonably require to retain sufficient documentation that is necessary to support any advice, reports, or opinions that we may provide.
9. This Agreement shall not apply to Confidential Information that:
10. Is in the public domain at the time it is acquired by us;
11. Enters the public domain after that, otherwise than as a result of unauthorized disclosure by us;
12. Is already in our possession prior to its disclosure to us; and is independently developed by us
13. This Agreement shall continue perpetually unless and to the extent that you may release it in writing.
14. We acknowledge that the Confidential Information will not form the basis of any contract between you and us.
15. We warrant that we are acting as principal in this matter and not as agent or broker for any person, company, or firm.
16. We acknowledge that no failure or delay by you in exercising any right, power or privilege under this Agreement shall operate as a waiver thereof nor shall any single or partial exercise thereof or the exercise of any other right, power, or privilege.
17. This Agreement shall be governed by and construed in accordance with Indian law and any dispute arising from it shall be subject to the exclusive jurisdiction of the Thrissur courts.

We have read this Agreement fully and confirm our agreement with its terms

Yours sincerely

[Signature & Stamp of the Company]

Authorised Person Name:

Designation