TRIPURA STATE ELECTRICITY CORPORATION LIMITED

(A Govt. of Tripura Enterprise)

Office of the Additional General Manager (DP&C)
Bidyut Bhavan, North Banamalipur, Agartala, Tripura

BID DOCUMENT

DNIT NO : AGM(DP&C)/TSECL/RDSS/LR/IT-OT/09, Dated: 17.12.2022

Name of Work : **Appointment of Cloud Service Provider / Managed Service Provider to host existing ERP System of TSECL along with Design, Implementation & Support of Project Execution Management System (PEMS) under Revamped Distribution Sector Scheme (RDSS).**

Estimated Cost : **Rs. 2,65,02,000/-**
(Rupees Two Crore Sixty Five Lakh Two Hundred only)

Time for Completion : **3 Years & 6 months (42 Months)**

Date of Release of RFP/ NIT	***19th December, 2022***
Date & Time of Pre-Bid Meeting	***27th December, 2022 at 11:30 AM***
Deadline for Submission of Bid	***9th January, 2022 up to 05:00PM***
Date & Time of Opening of Technical Part of Bid	***10st January, 2022 at 03:30 PM***

Technically Sanctioned and Administrative Approval provided for **Rs. 2,65,02,000/-** (Rupees Two Crore Sixty Five Lacs and Two Thousands only) including GST vide T.S. NO - AGM (DP&C)/ TSECL/RDSS/LR/IT-OT/2022-23/62 Dated: 19/12/2022.

This documents contains 141 (One Hundred and Forty One) Pages including the Cover page.

Regd. Office: O/o The Addl. General Manager (DP&C), TSECL
Bidyut Bhaban, North Banamalipur, Agartala, West Tripura, Pin: 799001
Tele. 0381-222-8001 / 232-5843 / 222-6613, CIN: - U40101TR2004SGC007434
Website: www.tsecl.in // Email: project.distribution@tsecl.in

NOTICE INVITING E-TENDER

(NATIONAL OPEN COMPETITIVE PROCUREMENT)
(SINGLE STAGE TWO ENVELOPE BIDDING)

DATE OF ISSUANCE OF NIT **: 17/12/2022**

FUNDING **: Revamped Distribution Sector Scheme (RDSS)**

1.0 Addl. General Manager, (DP&C), TSECL, Agartala invites the tender on behalf of TSECL for the following work from eligible and resourceful contractors/firms having sufficient credential and financial capability for execution of works of similar nature through **Electronic tendering (e-Tendering).**

Item No.	Name of Work and NIT No.	Estimated Value	Earnest Money/ Bid Security / Tender Cost	Completion period
1	**Appointment of Cloud Service Provider / Managed Service Provider to host existing ERP System of TSECL along with Design, Implementation & Support of Project Execution Management System (PEMS) under Revamped Distribution Sector Scheme (RDSS).** **NIT/ Spec No:- AGM(DP&C)/TSECL/RDSS/LR/IT-OT/09, Dated: 17.12.2022**	**Rs. 2,24,59,322/- excluding GST**	**Rs. 4,49,200.00/-** **Rs.10,000.00/- (Including all taxes)**	**3 Years & 6 Months (42 Months)**

i. Earnest money deposit shall be 2% of the Estimated Value put to tender subject to maximum of Rs.5(Five) Crore,

ii. If the offer is submitted with inadequate Earnest money i.e. less than 2% of the estimated value put to tender subject to maximum of Rs.5(Five) Crore the bid shall be rejected.

2.0 This NIT for the above work will appear in National and Local Newspapers. This shall also be available on Tripura State Electricity Corporation Limited website **at www.tsecl.in** from **17-12-2022.** The complete Bidding Documents shall be available at Government e-procurement portal https://tripuratenders.gov.in from **17-12-2022.** Interested bidders can download the Bidding Documents and commence preparation of bids to gain time.

3.0 Eligible bidders shall participate in tender online through the government e-procurement portal at https://tripuratenders.gov.in.Tender shall be uploaded/submitted in a Single Stage Two-Envelope Bidding system:

(a) Bid Envelop-I (Technical bid)

(b) Bid Envelop-II (Financial bid**)**

4.0 Bidders willing to take part in the process of e-tendering are required to obtain a valid Class 2/Class 3 **Digital Signature certificate (DSC)**, from any of the of the certifying authorities, enlisted by Controller of Certifying Authorities (CCA) at http://cca.gov.in. After obtaining the Class 2/3 Digital Signature Certificate (DSC) from the approved CA, Bidders shall enroll themselves in the Tripura Government e-procurement web site at https://tripuratenders.gov.inand obtain User ID and Password for the purpose of bidding.

5.0 Critical Dates:

1.	Completion period:	**3 Years & 6 Months (42 Months)**
2.	Date of Publishing of tender :	**17-12-2022**
3.	Period of downloading of Bidding Documents at tripuratenders.gov.in:	From: **19-12-2022**
		To: **08-01-2023**
4.	Period of Seeking Clarifications :	From: **19-12-2022**
		To: **03-01-2023**
5	Time and date of Pre-Bid Meeting:	**27-12-2022 at 11.30 A.M.**
6.	Place of Pre-Bid Meeting:	O/o: Addl.General Manager (DP&C), TSECL, Bidyut Bhaban, Banamalipur, Agartala, West Tripura, Pin: 799001, Ph. 0381-230 7433, Fax: 0381 232 5345.
7	Deadline for submission of EMD, Integrity Pact, Cost of tender and all requisite documents (Hard Copy)	**09-01-2023 up to 05:00 PM**
8	**Deadline for online Bidding:**	**09-01-2023 up to 05:00 PM**
9	Time and Date of Opening Technical Bid/Bids:	**10-01-2023 at 03:30 PM**
10	Time and Date of Opening Price/Financial Bid:	To be notified after Technical Evaluation
11	Place of Opening Bids:	O/o: Addl. General Manager (DP&C), Corporate Office, Bidyut Bhaban, Agartala, West Tripura, Pin: 799001, Ph. 0381-230 7433, Fax: 0381 232 5345.
12.	Bid Validity:	180 (One Hundred and Eighty) Days from the date of Opening of Technical Bid.
13.	Officer inviting Bids (TSECL):	O/o: Addl. General Manager (DP&C), Corporate Office, Bidyut Bhaban, Agartala, West Tripura, Pin: 799001, Ph. 0381-230 7433, Fax: 0381 232 5345.

6.0 **Scope of Work**:

The scope of work under the subject package includes **Appointment of Cloud Service Provider / Managed Service Provider to host existing ERP System of TSECL along with Design, Implementation & Support of Project Execution Management System (PEMS) under Revamped Distribution Sector Scheme (RDSS).**

Scope of work given above is only indicative. The detailed scope has been described in the SBD and as per schedule of supply of item(s)/BOQ& services.

7.0 Bidding will be conducted through the Global Open competitive bidding procedures as per the provisions of ITB/BDS and the contract shall be executed as per the provisions of the Contract.

8.0 The detailed Qualifying Requirements (QR) is given in the Standard Bidding Documents (SBD).

9.0 Earnest Money Deposit amounting to 2% (Two Percent) of the estimated cost put to tender i.e. **4,49,200.00/-**.The Earnest Money Deposit shall be submitted by Demand Draft (DD)/ Bank Guarantee (BG) from any Scheduled Bank guaranteed by Reserve Bank of India favoring TRIPURA STATE ELECTRICITY CORPORATION LIMITED payable at Agartala in the concerned format prescribed in the Bid Document. The Bid Security shall be valid for ninety (90) days beyond the original validity period of the Bid, or beyond any period of extension if requested. Earnest Money Deposit in any other form or amount will not be accepted.

Tender Fee shall be submitted only in the form of Demand Draft on any Scheduled Bank guaranteed by Reserve Bank of India favouring TRIPURA STATE ELECTRICITY CORPORATION LIMITED payable at Agartala.

10.0 Submission of original copies of documents of Tender Cost and Earnest Money Deposit and Integrity Pact and Hard copy of all credential documents:

The Bidder shall have to submit **hard copy of the documents as specified in the Bid Document**, i.e. has to deposit both the original Demand Drafts/ Bank Guarantee (BG) against related Tender Fee and EMD (Bid Security) in a sealed envelope including Integrity Pact depicting NIT No. and the Bidders Name & Address at "O/o Addl.General Manager (DP&C), Tripura State Electricity Corporation Limited, Corporate Office, Bidyut Bhaban, Agartala, West Tripura, Pin: 799001." on or before **05:00 P.M of 09-01-2023.** Scanned copies of all other original documents / certificates / annexure /declarations / undertakings / formats are to be uploaded in the e-tender portal by the bidder as a part of the Techno-commercial part of the bid against this tender and the same shall be submitted in original before signing of the contract if the work is awarded.

11.0 Power of Attorney, if given to authorized signatory for signing the Contract Agreement, shall be made in an INDIA NON-JUDICIAL STAMP OF Rs.100.00 (Rupees one hundred) only.

12.0 On award of work the successful bidder shall have to deposit a contract performance **guarantee (CPG) equivalent to 3%** of the LOA value / Supply order value in the shape of Demand Draft in favour of Tripura State Electricity Corporation Limited from any schedule Bank guaranteed by Reserve Bank of India, payable at Agartala or in the shape of Bank Guarantee from a Public sector / scheduled Indian Bank guaranteed by Reserve Bank of India.

12.1 Extension of bank guarantee for performance of the contract shall be extended as & when asked by the Engineer in charge to keep the currency of the contract alive. In the event of failure on the part of agency to extend the bank guarantee before expiry of the bank guarantee submitted, the same shall be en-cash without showing the reason thereof.

13.0 The acceptance of Price bid /financial bid shall be subjected to acceptance of Tender fee & EMD.

14.0 The Bidding Documents are meant for the exclusive purpose of bidding against this specification and shall not be transferred to any other party or reproduced or used otherwise for any purpose other than for which they are specifically issued.

15.0 Downloaded NIT, Bid Document are to be uploaded back and digitally signed as a part of technical bid, and as a proof of acceptance of all terms and conditions in NIT and Bid Document.

16.0 The intending bidder has to quote all items as per BOQ, part quoting rate will not be entertained and will be rejected.

17.0 Submission of Bids**:**

Bids are to be submitted online through the website, and as, stated in **Clause 1.0 and 2.0**. All the Bidding documents (SBD, Scan copy of tender fee) uploaded by the TSECL form an integral part of the contract. Bidders are required to upload these bidding documents as asked for in the Bid, through the above website and within the stipulated date and time mentioned in the Tender.

Tenders are to be submitted in two envelops at a time for each work, one for Technical Proposal and the other for Financial Proposal. The Bidder shall carefully go through the requirements and prepare the required documents to be uploaded.

In Technical Bid, Bidder shall have to submit/upload the entire requisite document as specified in the NIT and SBD (NIT, SBD, Scan copy of tender fee and EMD, All forms/Amendments/Formats/Annexure with supporting documents/certificates /Financial, Tax related document, machinery & manpower details specified in the Bid Document etc.

In, Financial Bid, Bidder shall upload BOQ as part of the financial Bid.

The bidder shall scan all the documents before uploading and all scanned documents shall be of 100 dpi resolution in Portable Document Format (PDF).The scanned documents shall be uploaded in the designated locations of Technical Bid and Financial Bid, as prompted by the e-Procurement website.

The Bidder needs to fill up their name and rates for all the items and in the designated Cells of the downloaded BOQ for the related work, and upload the same in the designated location of Financial Bid. The documents uploaded are virus scanned and digitally signed using the Digital Signature Certificate (DSC). Bidders shall specially take note of all the addendum/corrigendum related to the tender and upload the latest documents as part of the tender.

(Technical Bid) :

The Technical Bid/Bid Envelop-I should contain scanned copies and/or declarations in the following standardized formats.

A. My Document (Non-Statutory):

All the below-mentioned documents/certificates are to be uploaded with digital signature in the '**MyDocument**' folder option available after login in the e-procurement portal https://tripuratenders.gov.in. Bidders are requested to scan the necessary documents in **100 dpi** resolution into PDF. 'My Document' shall be populated prior to real time bidding and during real time bidding, uploaded documents/certificates in the 'My Document' are to be appropriately included (Checked)for incorporation in the Bid.

An indicative organization of 'My Document' folder and the related documents are indicated here under.

Sl.	Folder Name	Documents to be uploaded
1.	Manufacturing License / Registration of firm	**Company Details:** Registration of the firm/Partnership deed/ Articles of Association/ MOA Empanelment letter from MeitY
2.	DNIT Documents	Corrigendum, if published
3.	Machinery/Factory Details	Company Profile, Machinery & Manpower in possession of the firm
4.	Tax related document	GST Registration certificate IT PAN, TAN
5.	Financial details	Audited Balance Sheets of last five financial years with auditor's certificate regarding annual turnover from contracting business in each year.
6.	Misc. document	Any other documents found necessary (Such as Proof for authorized Signatory: Letter from Company Secretary providing due authorization to the signatory, Manufacturers Authorization Form/ Certificate (MAF))

B. Statutory Documents:

Along with the above mentioned non-statutory documents/certificates, Bidders shall submit / upload the following statutory documents, during real time bidding

1. Scanned copy of Tender Fee and EMD in single PDF.
2. Scanned copy of Integrity Pact as being submitted by the bidder
3. NIT.
4. SBD (Bid Document).
5. All annexure/ formats/certificates including supporting documents/certificates in support of qualifying requirement other than mentioned in My Document specified in the Bid Document in single PDF.

Note : Bidders are requested to scan the necessary documents/certificates in **100 dpi** resolution into PDF.

(Financial Bid):-

Documents to be submitted in the Financial Bid are:

BOQ (Bill of quantity /Price schedule).

Note: Bill of Quantity (BOQ) i.e. Price schedule, which is the Rate quoting sheet in MS excel shall be downloaded, filled up properly and uploaded back in the financial bid after digital signing. The Bidder shall always open the BOQ sheet with Macros Enabled. The Bidder shall quote rates in numerical figures only, for all items in the Bill of Quantity (BOQ).

18.0 **BOQ (Price Schedule) TAMPERING**: The provided BOQ (Price schedule) in the Tender is meant for downloading in the Bidders client machine, for entering the relevant fields meant for rates & bidder's particulars and finally uploading in the Financial Bid. The BOQ Excel Sheet is Macro enabled and working with the Sheet requires the Macro to be allowed/ enabled to run.

Bidders are hereby warned not to tamper the Excel Sheet, make copies and work in a copied Sheet or break through the default Work-Sheet Security. Such BOQs with stated violations will be treated as Tampered BOQs and Bids uploaded with Tampered BOQs will be summarily rejected.

19.0 Bidders are allowed to bid 24x7 till the time of Bid closing, with option for Re-Submission, wherein only their latest submitted Bid will be considered for evaluation. The e-Procurement website will not allow any Bidder to attempt bidding, after the scheduled date and time.

20.0 For any clarifications related to NIT/Bid Document/e-procurement, bidder(s) are requested to contact:

O/o The AGM (DP&C),

Tripura State Electricity Corporation Limited,

Corporate Office, BidyutBhaban,

Agartala-799001, Tripura (West).

Email: project.distribution@tsecl.in, Ph. 0381-230 7433, Fax: 0381 232 5345.

21.0 Addendum/ amendments /corrigendum:

Before the last date for submission of Tenders, the TSECL may modify any of the Contents of the Tender Notice, Tender documents by issuing amendment / Addendum/corrigendum.

Any addendum/amendments/corrigendum issued by the TSECL shall be part of the tender Document and it shall be published in the e-procurement portal at https://tripuratenders.gov.in. However, TSECL shall bear no responsibility or liability arising out of non-receipt of the same in time or otherwise. Bidders are requested to visit the site frequently to check whether there is any related Corrigendum(s) or not.

TSECL reserves the right to cancel/withdraw this invitation for bids without assigning any reason and shall bear no liability whatsoever consequent upon such a decision.

Sd/-

Addl. General Manager (DP&C)
Tripura State Electricity Corporation Limited
Corporate Office, Bidyut Bhaban
Agartala, Tripura (West)

Contents of the Tender Document

Contents

1. Introduction

Tripura State Electricity Corporation Limited (TSECL) wishes to leverage the benefit of Cloud services to achieve vertical & horizontal scalability to address its growth plan without impacting on performance and without locking to a specific technology. TSECL has already implemented its Enterprise Resource Planning (ERP) covering three modules of Finance, Human Resources and Material Management under Integrated Power Development Scheme (IPDS) of Government of India. For this, the implementing agency has been selected and the FMS is running now. Now TSECL intends to appoint a Cloud Service Provider (CSP) or a Managed Service Provider (MSP) for deployment/hosting of ERP application on Enterprise Cloud Environment along with implementation & support of one standalone web-based application on Project Execution Management System (PEMS) as provided in this RFP. There are three different environments envisaged for cloud services namely Development, Quality and Production.

About Tripura State Electricity Corporation Limited (TSECL)

The Power Supply industry in Tripura was under the control of the Department of Power, Government of Tripura till 31st December 2004. The Department of Power, Government of Tripura, was entrusted with Generation, Transmission, and Distribution including Rural Electrification since inception. The Department of Power had remained a beneficiary constituent of North Eastern Regional Electricity Board. Tripura State Electricity Corporation Limited had started functioning w.e.f. 1st January 2005. Subsequently TSECL has taken over the entire existing network along with asset of erstwhile Department of Power for operating and maintaining the power supply industry in the State of Tripura. The main functions of TSECL are generation, transmission and distribution so as to ensure quality power supply to its consumers at affordable rates for the entire state of Tripura. TSECL has taken initiative for electrification of all villages and towns in the state and is also progressing towards electrification of all households. The area of operation under TSECL includes all the districts in Tripura. The total area covered is around 10491.69 square kilometers and the population of area covered by TSECL is 36.71 Lakhs approx. TSECL caters to a total of more than 8.18 Lakhs (approx.) consumers. Recently a generation company in the name of "Tripura Power Generation Limited" (TPGL) has been constituted and all assets relating to Generation projects owned by TSECL is being transferred to TPGL. However, TPGL has not started complete independent operations till date and most of the central the functions of generations are looked after by TSECL.

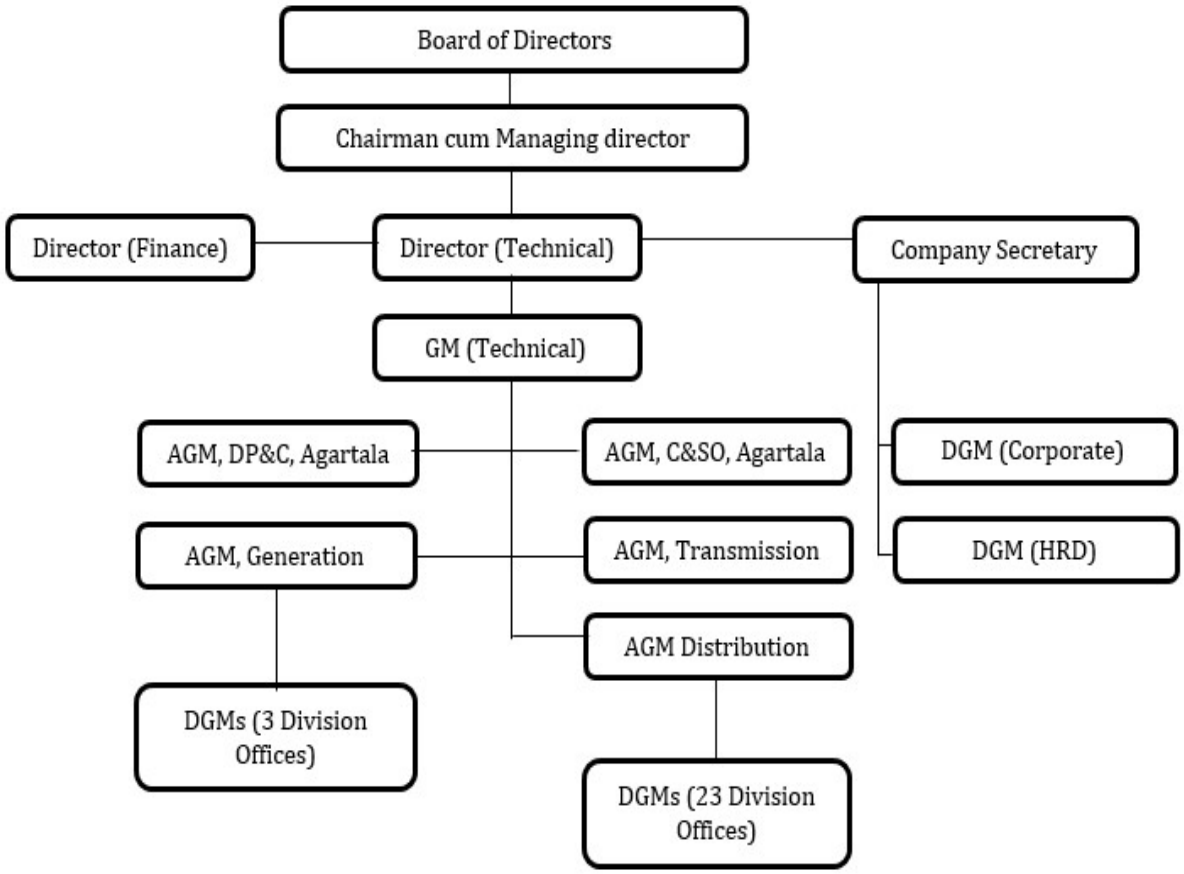
Functions of Tripura State Electricity Corporation Limited (TSECL)

The main business functions of TSECL can be classified as:

1. Managing revenue, financing arrangements, preparation of cashbooks, financial approvals and budgeting apart from employee related payables like salary, advances, pension, gratuity, insurance and other allowances.
2. All employee related activities such as recruitment, training & development, performance appraisal (Annual Confidential Reports), promotions, higher pay scale, disciplinary cases, transfers and retirement.
3. Regulatory activities like filing of tariff and true-up petitions, attending hearings, responding to queries
4. Project planning, feasibility study, load flow studies, energy audit, system strengthening and augmentation activities
5. Execution and monitoring various turnkey projects, activities related civil construction

6. Procurement of material and services
7. Inventory management activities such as inspection, receipt and issue of materials.

Organization Structure of Tripura State Electricity Corporation Limited (TSECL)



A separate entity called Tripura Power Generation Limited was constituted to look after the generation business. The transmission and distribution businesses are looked after by TSECL itself. The detailed list of business location of TSECL are provided below:

Business	Number of offices of TSECL
Electric Division (Generation)	3
Electric Division (Transmission)	4
Distribution	
Electric Circle	9
Electric Division	18
Electric Sub-Division	67
Distribution Franchisee Division	5

Objective of Procuring Cloud Services

TSECL wishes to procure Cloud services to host the ERP system which is under implementation by M/s Idea Infinity IT Solutions Pvt Ltd., Bangalore.

TSECL, through implementation of ERP system, wants to make its business processes efficient, more robust and reliable. Organization's aim is also to provide best services to its consumers. Integrating its business processes across divisions and sub-divisions will ensure that the seamless exchange of information will result in better future planning and decision making. TSECL's key objectives for implementing ERP are:

1. Eliminating the requirement of making multiple entries for a single change.
2. Ensuring transparency and legitimacy of data.
3. Provide real-time data to the senior management to facilitate quick response and better decision making.
4. Protection of sensitive data by consolidating multiple security systems into one.
5. Overhauling the current business functions thereby standardizing and automating these functions to reduce human intervention.
6. Better inventory control and tracking as well as enabling standard coding norms for assets.
7. Enabling a single common process across all divisions and sub-divisions of TSECL.

Overview of the Existing ERP System

TSECL has already implemented ERP system across its three business functions- Finance and Accounts, Human Resource Management and Material Management. The ERP modules implemented have been decided as per IPDS guidelines. These modules are as mentioned below:

S. No.	Module	Abbreviation
1	Financial Management System	FMS
2	Human Resource Management and Payroll including Employee Self Service (ESS)	HRMS
3	Material Management System	MMS

2. Instruction to Bidder (ITB)

1.0 GENERAL

1.1. **General Instructions**

Bidders are to satisfy themselves by actual site visit for the assessment of the opportunity with regard to the prevailing business processes, IT infrastructure, conditions of work, requirements of purchaser etc. before submission of bid. No claim on this account will be entertained at any stage. The owner will not reimburse any expense for such visit.

1.2. **Eligible Bidders**

The bidder must be firm/ company/ partnership firm registered in India under the Indian Companies Act, 1956/2013 under Ministry of Corporate Affairs, Govt. of India.

CSPs/MSPs or authorize Partners of CSP Product Vendors are only allowed to participate. The MSP will have to provide written consent of the original CSP to associate with the MSP for this particular opportunity/RfP.

The Bidder in order to be eligible to participate in the tendering process, must meet all the mandatory requirements as per the parameters defined in Section 7: Evaluation Details.

1.3. **Lack of information to bidder**

The bidder shall be deemed to have carefully examined the Bid document to his entire satisfaction. Any lack of information shall not relieve the bidder of his responsibility to fulfill his obligation under the bid. If bidder has any queries relating to the bid document, then he can send the queries before the Pre-Bid Meeting.

1.4. **Eligible Goods and Related Services**

For purposes of this Clause, the term "Goods" means all software including ERP database, application, middleware and any other related software and licenses that the Bidder is required to supply to the Purchaser under the Contract; and "Related services" means ERP Implementation & Support and includes services such as insurance, installation, configuration, implementation, training, maintenance and other related/ancillary services that may be required to execute this Contract.

In case Bidder does not manufacture or produce the Goods it offers to supply, it shall submit the Original Equipment Manufacturer's Authorization Certificate to demonstrate that it has been duly authorized by the manufacturer or producer of the Goods to supply these Goods.

2.0 CONFLICT OF INTEREST

2.1. The ERP Implementing Agency and ERP PMU Agency and any other entity affiliated with them, who were associated with the preparation of this Tender document shall not participate in any manner in the bid.

2.2. The bidder must submit a certificate of "No Conflict of Interest" through authorized signatory, confirming that there would be no conflict of interest with TSECL. Bids of any Bidder may be rejected if a conflict of interest between the bidder and TSECL is detected at any stage.

3.0 COST OF BIDDING

The Bidder shall bear all the costs and expenses associated with preparation and submission of its Bid including post-bid discussions, technical and other presentation etc. and the TSECL shall in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

4.0 THE BIDDING DOCUMENT

4.1. Contents of Bidding Documents

The goods and services required, bidding procedures and contract terms are as prescribed in the Bidding Documents.

In addition to the Invitation for Bids, the Bidding Documents is a compilation of the following sections:

a. Section – I:- Introduction

b. Section – II:- Instructions to Bidder

c. Section – III:- Bid Data Sheet

d. Section – IV:- General Conditions of Contract (GCC)

e. Section – V:- Special Conditions of Contract (SCC)

f. Section – VI:- Scope of Work

g. Section – VII:- Evaluation Details

h. Section – VIII:- Mandatory Forms

i. Section – IX:- Bidding Forms

j. Section – X:- Contract Forms

k. Section – XI:- Bid Check List

m. Section – XII: - Annexure 1 (Service Level Agreement)

n. Section – XIII:- Annexure 2 (Workflow of PEMS)

4.2. Understanding of Bidding Documents

A prospective Bidder is expected to examine all instructions, forms, terms and specifications in the Bidding Documents and fully inform himself as to all the conditions and matters which may in any way affect the scope of work or the cost thereof. 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 shall be at the Bidder's risk and rejection of Bid.

5.0 CLARIFICATIONS ON BIDDING DOCUMENTS

5.1. If prospective Bidder finds discrepancies or omissions in the specifications and documents or is in doubt as to the true meaning of any part or requires any clarification on Bidding Documents should make the request / notify the Tender inviting Authority of TSECL in writing. The concerned authority of TSECL shall respond in writing to any request for such clarification of the Bidding Documents, which it receives not later than as mentioned in section -I prior to the deadline for submission of bids stipulated in tender notice. Written copies of the response (including an explanation of the query but without identifying its source) shall be sent to all prospective bidders who purchased the tender document.

5.2. Verbal clarification and information given from any offices of TSECL or its employee(s) or representative (s) shall not in any way be binding on TSECL.

6.0 CORRIGENDUM/AMENDMENT TO BIDDING DOCUMENTS

6.1. At any time prior to the deadline for submission of bids, TSECL may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the Bidding Documents by amendment (s).

6.2. The amendment(s) will be published in the e-Tender portal at **http://www.tripuratenders.gov.in.** Registered Bidders shall be notified of the related Corrigendum(s) by e-mail. However, TSECL shall bear no responsibility or liability arising out of non-receipt of the same in time or otherwise. Bidders are requested to visit the site frequently to check whether there is any related Corrigendum or not.

6.3. In order to afford prospective bidders reasonable time to take the corrigendum/amendment into account in preparing their bids, TSECL may, at its discretion, extend the deadline for submission of bids.

6.4. Such corrigendum/amendment, clarifications, etc shall be binding on the bidders and shall be given due consideration by the bidders while they submit their bids and invariably enclose such documents as a part of the Bid.

7.0 PREPARATION OF BIDS

Language of Bid

The Bid prepared by the Bidders and all correspondence and documents relating to the bid, exchanged by the Bidder and TSECL, shall be written in English language, provided that any printed literature furnished by the bidder may be written in another language so long as accompanied by an English translation of its pertinent passages. Failure to comply with this may disqualify a bid. For purposes of interpretation of the bid, the English translation shall govern.

8.0 LOCAL CONDITIONS

8.1. It shall be imperative on each bidder to fully inform him of all local conditions and factors, which may have any effects on the execution of the contract covered under these documents and specifications. **The Owner shall not entertain any request for clarification from bidders, regarding such local conditions**.

8.2. It must be understood and agreed that such factors as above have properly been investigated and considered while submitting the proposals. No claim for financial adjustment to the Contract awarded under these specifications and documents shall be entertained by TSECL. Neither any change in the time schedule of the Contract nor any financial adjustments arising thereof shall be permitted by TSECL.

9.0 DOCUMENTS COMPRISING THE BID

The Bid shall be submitted in 2(two) parts, post registration in the http://www.tripuratenders.gov.in, as under:

Part-I: Envelop-I (Technical Bid):

9.1. Containing Tender Fee & Earnest Money as per the stipulations described under the title "Notice Inviting Tender" of Section 1 in this Bid Document. No financial aspect will be entertained in technical bid.

9.2. Containing Documentary Evidence of the Bidder in fulfilling the qualifying requirements as indicated hereunder in brief and in detail in Clause 7.2 of Section 7 (Evaluation Details) of the NIT / Bid Document.

9.3. Containing Bidder's Technical Proposal as per technical specification of Section-7 Evaluation Details along with his Commercial Terms, Payment Terms in conformity with the Form No, 10 'Price Bid' of the Section 8 Bidding Forms of this bidding document.

Bid Envelop-II (Price Bid/Financial Bid):

9.4. Only the bidders who have met the pre-qualification shall be considered for opening of Price bid/Financial Bid.

The Price Bid/ Financial Bid shall be consisting of the following documents:

Bill of Quantity (BOQ) i.e. the Price Bidding Schedule - to be downloaded.

Regarding **Bill of Quantity** mentioned as above (BoQ), the Bidder shall download the BOQ file in XLS format from the Tender document. All cells of the XLS document will be protected except the field (Bidder's Name and Rates only in figures), the Bidder is expected to fill in. The BoQ XLS document shall contain bundled Macros which shall have to be enabled for automatic calculations and "figure to word conversions".

NB: In addition to the composition of the **Technical Bid** regarding the documents to be supplied, the Bidder may also supply additional documents in either of this Bid, as Non-Sensitive documents, by scanning the related documents in PDF format (100 dpi scan resolution) and saving them in Bidder's "My Document" before-hand. The Bidder may suitably use any additional document from his "**My Documents**" for proper justification of his **Technical Bid.**

10.0 SCOPE OF THE PROPOSAL

10.1 The scope of the proposal shall cover all the items specified under **Section 6: Scope of Work**.

10.2 Bids containing deviations from provisions relating to the following clauses shall be considered as '**non-responsive'**:

a) Price Basis and Payments & Price Adjustment
b) Bid Guarantee
c) Contract Performance Guarantee
d) Liquidated Damages: General Condition of Contract
e) Payment

The determination of a Bid's responsiveness will be based on the contents of the Bid itself without recourse to extrinsic evidence.

10.3 The selected bidder shall be responsible for managing and controlling the underlying Cloud Infrastructure including operating systems, storage, network, security, etc.

10.4 Bids not **covering the entire Scope of Work** as mentioned above and in detail in Section 6: Scope of Work shall be treated as incomplete and hence rejected.

11.0 BID PRICE

The Bidder shall quote unit rates in the downloaded BOQ XLS file and upload the same in Financial Part of the Tender.

12.0 ALTERNATE PROPOSALS

Bidder shall submit offers that comply with the requirements of the bidding documents, **including** the basic technical design as indicated in the specifications. Alternatives will not be considered.

13.0 PRICE BASIS AND PAYMENTS

13.1 The bidders shall quote in their proposal price for the entire Scope of Supply covered under the Technical Specification as required in the Clause 9.13 Price Bid of the Section 9 Bidding Forms this Bid Document.

13.2 Bidder shall indicate Bid prices in Indian Rupees only.

14.0 TAXES AND DUTIES

14.1. Prices shall be quoted in the 'BOQ/Price Bid' for the services to be provided as per scope of work described in Section 6 of the bid document, with applicable GST. Quoted prices shall be firm and inclusive of all applicable tax and duties.

14.2. Goods and Services Tax (GST) as applicable on twenty-eight (28) days prior to deadline for submission of bids shall be mentioned in the BoQ of Price Bid. In case the bidder fails to submit GST rates against any items, the applicable statutory rate shall be assumed to be included in the total price quoted and no escalation of cost due to errors in quoting of cost on account of GST shall be permitted.

14.3. Applicable GST shall be reimbursed by TSECL on submission of actual documentary proof based on tax invoices raised by the contractor.

14.4. Statutory variation in Taxes & duties after twenty-eight (28) days prior to deadline for submission of bids and during the scheduled completion period will be adjusted / reimbursed against production of documentary evidence.

14.5. Income Tax as admissible will be deducted at source for which necessary TDS certificate will be issued".

14.6. Bidder shall be reimbursed for payment of any statutory duty/tax/levy including interest and/or new taxes or an increase in the rates of existing taxes or any other sum, if any payable in respect of any sales tax and/or state or central levy.

15.0 TIME SCHEDULE

15.1. The entire infrastructure works (handover to TSECL after completion of all installation and configuration activities) as per the scope of contract should be completed within 90 (Ninety) days from the date of issuance of LOA. Thereafter the contract period shall be for 3 years 6 months (42 Months) from the commencement of operations.

15.2. The implementation of the PEMS shall be completed within 3 months from the date of issue of the LOA (including the stabilization period) and 42 months of FMS support.

15.3. The basic consideration and the essence of the Contract shall be strict adherence to the time schedule for performing the specified supply/works.

15.4. TSECL reserves the right to request for a change in the supply/work schedule during post-bid discussion with successful bidder.

15.5. The successful Bidder shall be required to submit detailed PERT CHART and finalize the same with TSECL, as per the requirement of completion schedule.

16.0 CONTRACT QUALITY ASSURANCE

16.1. The Bidder shall include in his proposal, the quality assurance program containing the overall quality management and procedures which he proposed to follow in the performance of the supply/works during various phases, as detailed in relevant clause of the General Technical Conditions.

16.2. At the time of award of Contract, the detailed quality assurance programme to be followed for the execution of the contract shall be mutually discussed and agreed to and such agreed programme shall form part of the contract.

17.0 INSURANCE

The bidder's insurance liabilities pertaining to the Scope of supply/Work is detailed out in clauses titled insurance in General Terms & Conditions of Contract. Bidder's attention is specifically invited to these clauses. The bid price shall include all the cost in pursuance of fulfilling all the insurance liabilities under the Contract.

18.0 BRAND NAMES / NAMING CONVENTIONS

18.1. The specific reference in these specifications and documents to any material/ equipment, module name, implementation phase by brand name, make or catalogue number shall be construed as establishing standards of quality and performance and not as limiting competition.

18.2. The Bidder shall note that standards for workmanship, material and equipment and reference to brand name or catalogue numbers designated by the Owner in its Technical Specification are intended to be descriptive only and not restrictive. The Bidder may substitute alternative standards, brand name and/or catalogue numbers in its Bid, provided that it demonstrates to the Owner's satisfaction that the substitutions are substantially equivalent or superior to those designed in the Technical Specification.

19.0 BID GUARANTEE/ EARNEST MONEY DEPOSIT (EMD)

19.1. The Bidder shall furnish, as part of its Bid, earnest money for an amount as specified in the Notice Inviting Tender (NIT).

19.2. The earnest money is required to protect TSECL against the risk of Bidder's conduct, which would warrant the earnest money forfeiture pursuant to Para 19.7.

19.3. The earnest money shall be deposited in Indian rupees only.

19.4. Any bid not secured in accordance with para 19.1 and 19.3 above shall be rejected by TSECL as non-responsive.

19.5. The earnest money of the unsuccessful Bidders shall be discharged /returned as promptly as possible as but not later than 60 days after the expiration of the period of bid validity prescribed by the Owner.

19.6. The EMD of the successful bidder will be returned after submission of performance bank guarantee. Note: EMD will be submitted through net banking via e-tender portal and bank guarantee will be submitted in legal document.

19.7. The earnest money shall be forfeited:

a. If a Bidder withdraws its bid during the period of bid validity specified by the Bidder on the bid form; or

b. In case of a successful Bidder fails

i. to sign the contract; or

ii. to furnish the 'Contract Performance Guarantee'.

19.8. No interest shall be payable by TSECL on the above earnest money.

20.0 PERIOD OF VALIDITY OF BIDS.

20.1. Bids shall remain valid for 180 days after the date of bid opening prescribed by TSECL, unless otherwise specified in the accompanying. A Bid valid for a shorter period shall be rejected by TSECL as non-responsive.

20.2. In exceptional circumstances, TSECL may solicit the Bidder's consent to an extension of the period of Bid validity. The request and the response thereto shall be made in writing (including fax or email). The Earnest money provided under Section – 3 shall also be retained upto the extended period. No interest shall be payable by TSECL for retaining the earnest money upto the extended period. A Bidder may refuse the request without forfeiting the earnest money deposited by him. A Bidder granting the request shall not be required or permitted to modify his Bid.

21.0 FORMAT OF BID

21.1. Bids are to be submitted online through the website, and as, stated in Clause 8.0 of ITB of Section-II and as per NIT. All the documents uploaded by the Employer form an integral part of the contract. Bidders are required to upload all the bidding documents along with the other documents, as asked for in the Bid, through the above website and within the stipulated date and time mentioned in the Tender.

21.2. Tenders are to be submitted in two folders at a time for each supply/work, one for Technical Proposal and the other for Financial Proposal. The Bidder shall carefully go through the requirements and prepare the required documents to be uploaded.

21.3. The bidder shall scan all the documents before uploading and all scanned documents shall be of 100 dpi resolution in Portable Document Format (PDF).The scanned documents shall be uploaded in the designated locations of Technical Bid and Financial Bid, as prompted by the e-Procurement website.

21.4. The Bidder needs to fill up their name and rates for all the items and in the designated Cells of the downloaded BOQ for the related supply/work, and upload the same in the designated location of Financial Bid. The documents uploaded are virus scanned and digitally signed using the Digital Signature Certificate (DSC). Bidders shall specially take note of all the addendum/corrigendum related to the tender and upload the latest documents as part of the tender.

21.5. **Envelop-I (Technical Bid)**:

The Technical Bid/Bid Envelop-I should contain scanned copies and/or declarations in the following standardized formats.

My Document (Non-Statutory):

All the below-mentioned documents/certificates are to be uploaded with digital signature in the 'My Document' folder option available after login in the e-procurement portal **http://tripuratenders.gov.in.** Bidders are requested to scan the necessary documents in 100 dpi resolution into PDF. 'My Document' shall be populated prior to real time biding and during real time bidding, uploaded documents/certificates in the 'My Document' are to be appropriately included (Checked) for incorporation in the Bid.

An indicative organization of 'My Document' folder and the related documents are indicated here under.

Sl.	Folder Name	Documents to be uploaded
1.	Manufacturing License / Registration of firm	**Company Details:** Registration of the firm/Partnership deed/ Articles of Association/ MOA Empanelment letter from MeitY
2.	DNIT Documents	Corrigendum, if published
3.	Machinery/Factory Details	Company Profile, Machinery & Manpower in possession of the firm
4.	Tax related document	GST Registration certificate IT PAN, TAN
5.	Financial details	Audited Balance Sheets of last five financial years with auditor's certificate regarding annual turnover from contracting business in each year.
6.	Misc. document	Any other documents found necessary (Such as Proof for authorized Signatory: Letter from Company Secretary providing due authorization to the signatory, Manufacturers Authorization Form/ Certificate (MAF))

Statutory Documents:

After uploading the above mentioned non-statutory documents/certificates, Bidders shall submit the following, during real time bidding

1. Scanned copy of Tender Fee and EMD (Proof of Payment) in single PDF.

Note-1: If the company was set up less than five years ago, audited balance sheet for the no of years since inception is to be submitted.

Note-2: Bidders are requested to scan the necessary documents/certificates in **100 dpi** resolution into PDF.

Note-3: In any case if any document uploaded by the Bidders is/are not visible or cannot be opened for which tendering authority will not be responsible.

Note-4: Bidders shall have to produce original document as and when asked by the TSECL authority, for verification and authentication of submitted documents.

21.6. **Bid Envelop-II (Financial Bid)**:

BOQ.

Documents to be submitted in the Financial Bid are:

BOQ (Bill of quantity)/ Price schedule as specified in Section 9 of the RFP.

Note: Bill of Quantity (BOQ) i.e. Price schedule, which is the Rate quoting sheet in Ms-excel shall be downloaded, filled up properly and uploaded in the financial bid after digital signing. The Bidder shall always open the BOQ sheet with Macros Enabled. The Bidder shall quote rates in figures only, for all items in the Bill of Quantity (BOQ).

21.7. **BOQ (Price Schedule) TAMPERING**: The provided BOQ/ Price schedule in the Tender is meant for downloading in the Bidders client machine, for entering the relevant fields meant for rates & bidder's particulars and finally uploading in the Financial Bid. The BOQ

Excel Sheet is Macro enabled and working with the Sheet requires the Macro to be allowed/ enabled to run.

21.8. Bidders are hereby warned not to tamper the Excel Sheet, make copies and work in a copied Sheet or break through the default Work-Sheet Security. Such BOQs with stated violations will be treated as Tampered BOQs and Bids uploaded with Tampered BOQs will be summarily rejected.

21.9. Bidders are allowed to bid 24x7 till the time of Bid closing, with option for Re-Submission, wherein only their latest submitted Bid will be considered for evaluation. The e-Procurement website will not allow any Bidder to attempt bidding, after the scheduled date and time.

21.10. For any clarification related to NIT/SBD/e-procurement, bidder(s) are requested to contact:

O/O the Additional General Manager (DP&C),
Corporate Office, Bidyut Bhavan,
Tipura State Electricity Corporation Limited,
Banamalipur, Agartala-799001, Tripura (West).
e-mail: project.distribution@tsecl.in/agm.dpnc@tsecl.in
Ph. 9436471375,
Fax: 0381 2326613/ 0381 2319427;

22.0 SIGNATURE OF BIDS

22.1. Bid by a partnership must be furnished with full names of all partners and be signed with the partnership name, followed by the signature(s) and designation(s) of the authorized partner(s) or other authorized representative(s) and as per Section I & II of the BID.

22.2. Bids by Corporation / Company must be signed with the **legal name of the Corporation/Company** by the President, Managing Director or by the Secretary or other person or persons authorized to Bid on behalf of such Corporation / Company in the matter.

22.3. A Bid by a person who affixes to his signature the word 'President', 'Managing Director', 'Secretary', 'Agent', or other designation without disclosing his principal shall be rejected.

22.4. Satisfactory evidence of authority of the person signing on behalf of the Bidder shall be furnished with the Bid.

22.5. The Bidder's name stated on the proposal shall be exact legal name of the firm.

22.6. Bids not conforming to all the above requirements of para 21.0 above may be disqualified.

22.7. The original tender document shall be **digitally signed** by the bidder and will be uploaded during the e-Bid as part of the financial bid.

23.0 SEALING AND MARKING OF BIDS

The Bidder shall have to deposit both the proof of payment against related Tender Fee and EMD in a sealed envelope depicting NIT No. and the Bidders Name & Address at "O/O Additional General Manager (DP&C), Tripura State Electricity Corporation Limited, Corporate Office, Bidyut Bhaban, Agartala, Tripura (West).Pin: 799001" on or before 03/11/2022 at 11:00 am

24.0 DEADLINE FOR SUBMISSION OF BIDS

TSECL may, at its discretion, extend this deadline for the submission of Bids, in which case all rights and obligations of TSECL and Bidders previously subject to the deadline shall thereafter be subject to the deadline as extended.

25.0 MODIFICATION AND WITHDRAWAL OF BIDS

25.1. Withdrawal of Bid is permitted before tender closing.

25.2. The Bidder may Revise (modify) his Bid as many numbers of times he wants, till the point of Tender Closing. In such case, only his last modified Bid would be considered for evaluation.

25.3. A Bidder shall not withdraw, substitute, or modify its Bid after due date of bid submission.

26.0 OPENING OF BIDS BY TSECL

26.1. The Employer will designate Tender Opening Authority for each and every Bid separately, and the Technical bids will be opened online by them at the time and date, as specified in the NIT/ Standard Bid Documents.

26.2. All the Statements, Documents, Certificates, Demand Draft / Bank Guarantee etc. uploaded by the Bidders will be verified for technical evaluation. The clarifications and particulars, if any, required from the bidders, will be obtained by addressing the bidders directly. The technical bids will be evaluated against the specified parameters/ criteria mentioned in the BID, and in the same process as done in the case of conventional tenders. The technically qualified bidders will be identified and considered for their Financial Bid opening. The result of Technical Bids evaluation shall be displayed in the e-procurement portal and all the Bidders who have participated in the Tender will be able to access the same.

26.3. The Bidders or their authorized representatives may remain present at the time of opening of the tenders. Either the Bidder himself or one of his representatives with proper authorization only will be allowed at the time of tender opening. If any of the Bidders is not present at the time of opening of tenders, the tender opening authority will, on opening the tender of the absentee Bidder, read out and record the deficiencies if any, and this will be binding on the Bidder.

26.4. The Minutes of the Technical bid opening shall be recorded and signed by the Tender Opening Authority as well as Bidders or their Authorized Representatives present and the same shall be uploaded and can be accessed in the e-procurement portal.

26.5. The Price bids/Financial bids of all the technically qualified bidders will be opened by the concerned Tender Opening Authority at the specified date and time. The same can be tracked through the e-procurement portal by all the technically qualified bidders who participated in the tender. However, Qualified Bidders or their authorized representatives may remain present at the Price Bid (Financial bid) opening.

26.6. The Financial Bid's Item-wise Rates and total amount shall be read out, Minutes of the Bid opening shall be recorded, and the Bidder's signatures will be taken in the minutes. The result of financial bids (Price bids) evaluation shall be displayed in the e-procurement portal and Bidders can access the same.

26.7. The 'BOQ comparative chart' generated & displayed from the e-procurement portal, after the opening of financial Bid (which will be displayed as 'BOQ comparative chart' at financial bid opening summary page), will not be final.

26.8. Employer will prepare comparative Statement as per the decision of the Financial Bid Evaluation Committee in the Employer, which will be appropriately displayed in the e-procurement portal (this will be displayed at financial bid opening summary page).

26.9. The Price Bid /Financial Bid of the Unqualified Bidders will not be opened.

27.0 CLARIFICATION OF BIDS

During in the examination, evaluation and comparison of Bids, TSECL may, at its discretion, ask the Bidder for a clarification in writing before opening of Financial/Price bid. Once Financial/Price bid is opened no clarification will be done.

28.0 PRELIMINARY EXAMINATION

28.1. TSECL shall examine the Bids to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed and whether the Bids are generally in order.

28.2. The Bidder shall ensure that the prices furnished by him are complete. In the case of not quoting of rates of any item (supply) in the downloaded BOQ XLS file. TSECL shall be entitled to consider the QCBS selection criteria.

28.3. Prior to the detailed evaluation, TSECL shall determine the substantial responsiveness of each Bid w.r.t. Bidding Documents. For purpose of these Clauses, a substantially responsive Bid is one which conforms to all the terms and conditions of the Bidding Documents without material deviations. A material deviation is one which affects in any way the prices, quality, quantity or delivery period of the goods & services or which limits in any way the responsibilities or liabilities of the Bidder or any right of TSECL as required in these specifications and documents. TSECL determination of a Bid's responsiveness shall be based on the contents of the Bid itself without recourse to extrinsic evidence.

28.4. A Bid determined as not substantially responsive shall be rejected by TSECL and may not subsequently be made responsive by the Bidder by correction of the non-conformity.

28.5. TSECL may waive any minor non-conformity or irregularity in a Bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any Bidder.

29.0 PRICE BIDS

Total price bid will be all-inclusive of taxes, duties and levies.

30.0 AWARD CRITERIA

The technical Bids along with all the supporting documents shall be submitted in separate folder. Department will review the technical bids of the CSP to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at department's discretion. The CSP's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and technical evaluation framework. Each Technical Bid will be assigned a technical score out of a maximum of 100 marks. Only the bidders who get an aggregate technical score of 70% or more will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid and Bidder.

31.0 CONTACTING THE OWNER

Bids shall be deemed to be under consideration immediately after they are opened and until such time official intimation of award/rejection is made by TSECL to the Bidders. While the bids are under consideration, Bidders and/or their representatives or other interested parties are advised to refrain from contacting by any means, the Owner and/or his employees/representatives on matters relating to the bids under consideration. TSECL, if necessary, shall obtain clarifications on the bids by requesting for such information from any or all the Bidders, either in writing or through personal contacts as may be necessary. Bidders shall not be permitted to change the substance of the bids after the bids have been opened.

32.0 OWNER'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS

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

33.0 NOTIFICATION OF AWARD

33.1. Prior to the expiration of the period of bid validity and extended validity period, if any, TSECL shall notify the successful Bidder in writing by registered letter or FAX or email, to be confirmed in writing by registered letter, that his Bid has been accepted.

33.2. The Notification of Award / Letter of Award shall constitute the formation of the Contract.

33.3. Upon the successful Bidder's furnishing of Contract Performance Guarantee pursuant to Clause 35 of Section – 2. TSECL shall promptly notify each unsuccessful Bidder and will discharge its bid guarantee, pursuant to Clause 19 (Section – 2).

34.0 SIGNING OF CONTRACT

34.1. At the same time as TSECL notifies the successful Bidder that its bid has been accepted, TSECL shall send the Bidder the detailed Letter of Award.

34.2. Within 7(seven) days of receipt of the detailed Letter of Award, the successful Bidder shall convey in writing unconditional acceptance of the Letter of Award and shall attend the respective office of TSECL for signing the contract agreement.

35.0 CONTRACT PERFORMANCE GUARANTEE

35.1. On award of work the successful bidder shall have to deposit a contract performance guarantee (CPG), within 15 days of award of work, equivalent to 3% of the LOA value in the shape of Demand Draft in favor of Tripura State Electricity Corporation Limited from any schedule Bank guaranteed by Reserve Bank of India, payable at Agartala or in the shape of Bank Guarantee from a Public sector / scheduled Indian Bank guaranteed by Reserve Bank of India. The CPG shall remain valid for actual delivery period 45 (forty five) months plus a grace period of 3 (three) months (CPG is to be extended further subject to actual delivery period).

The Bank Guarantee should be executed in line with enclosed Proforma (Section 10. Contract Forms)) and on non-judicial stamp paper of Rs.100/=. **The CPG will be forfeited in case of non-compliance of order or failure to complete the order**. **Order will be**

cancelled for non-submission of CPG in time with forfeiture of earnest money. No claim shall be made against TSECL in respect of interest on CPG.

It shall guarantee the faithful performance of the Contract in accordance with the terms and conditions specified in these documents and specifications.

The contract performance guarantee submitted in the shape of Bank guarantee shall be valid up to guarantee period.

35.2. The Performance Guarantee shall cover additionally the following guarantees to TSECL:

a. The successful Bidder guarantees the successful and satisfactory operation of the equipment supplied under the Contract, as per the specifications and documents.

b. The successful Bidder further guarantees that the equipment supplied by him shall be free from all defects in design, material and workmanship and shall upon written notice from TSECL fully remedy free of expenses to TSECL such defects as developed under the normal use of the said equipment within the period of guarantee specified in the relevant clause of the General Terms and conditions.

35.3. The Contract Performance Guarantee is intended to secure the performance of the entire contract.

35.4. The Contract performance Guarantee submitted in the shape of demand draft shall be returned to the Contractor without any interest at the end of successful completion and commissioning of the supply against a Bank Guarantee of equivalent amount from any Public Sector / scheduled Indian Bank valid up to the Guarantee period. The Bank Guarantee such deposited shall be discharged after expiry of Guarantee period.

35.5. **The contract performance Guarantee shall be forfeited: -**

a) If the supplier fails to start the supply of Licensee and implementation work as per approved BAR CHART for reasons solely rest on him.

b) If the supplier left / suspends the supply without prior written intimation to the owner's Engineer in charge/ Nodal officer of the work stating the reasons for such suspension of supply.

c) If the supplier left / suspends the work of supply for reasons which are not acceptable to TSECL.

36.0 CORRUPT OR FRAUDULENT PRACTICES

36.1. TSECL expects the bidders / suppliers / contractors to observe the highest standards of ethics during the procurement and execution of such contracts. In pursuance of this policy, TSECL

a. defines, for the purpose of this provision, the terms set forth below as follows:

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

II. "Fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the owner 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 owner from the benefits of free and open competition.

b. Will reject a proposal for award if it determines the bidder recommended for award has engaged a corrupt or fraudulent practice in competing for the contract in question.

c. Will declare a firm ineligible, either indefinitely or for a stated period of time, if TSECL at any time determines that the firm has engaged in corrupt / fraudulent practices in competing for, or in executing the contract.

3. Bid Data Sheet (BDS)

Clause	Description
ITB 1.0	**The Purchaser is:** Tripura State Electricity Corporation Limited Bidyut Bhawan, Banamalipur, Agartala-799001, Tripura.
ITB 1.0	Selection of Cloud Service Provider / Managed Service Provider to host ERP system of TSECL Notice Inviting Tender Number: AGM (DP&C)/IT/002 Dated
ITB 1.2	Consortium/Joint Venture are **not** allowed to participate in the bidding process.
ITB 1.4	Bidder must produce a letter of authorization from the Original Cloud Service Provider (**Authorization Certificate**) in case it is a Managed Service Provider
ITB 4.0	**For Clarification purpose only, the Purchaser's address is:** Additional General Manager (DP&C) Tripura State Electricity Corporation Limited Bidyut Bhawan, Banamalipur, Agartala-799001, Tripura. Email id: agm.dpnc@tsecl.in
ITB 4.0	**Pre-bid Meeting schedule:** Time: 11:30 AM Date: 27th December, 2022 Venue: TSECL Conference Hall Bidyut Bhawan, Banamalipur, Agartala-799001, Tripura. **Tel:** 9436471375, **Fax:** 0381 2326613/ 0381 2319427; **E-mail:** agm.dpnc@tsecl.in Note: 1. All queries/suggestions related to the bid document need to be submitted using the format given in Section 9: Bidding Forms 7 days before the pre-bid meeting is scheduled. 2. Bidders need to send all queries / suggestions through email (PDF and MS Excel) at e-mail: agm.dpnc@tsecl.in

Clause	Description
ITB 5.0	The corrigendum(s)/ amendment(s) will be published in the e-Tender portal at http://www.tripuratenders.gov.in. Registered Bidders shall be notified of the related corrigendum(s)/ amendment(s) by e-mail. However, TSECL shall bear no responsibility or liability arising out of non-receipt of the same in time or otherwise
ITB 6.1	Language of this bid is English.
ITB 3.0	Cost of Tender Document INR Rs. 2,65,02,000/- (Rupees Two Crore Sixty Five Lakh Two Hundred only)
ITB 12.2	The bid currency is INR (Indian Rupee)
ITB 18.0	EMD: Rs. 4,49,200.00/-
ITB 19.0	**Bid Validity:** 180 Days
ITB 21.0	**Proof for authorized signatory shall be any of the following documents:** Board Resolution clearly stating that the signatory is authorized to sign and submit the proposal for the RFP. OR Letter from Company Secretary providing due authorization to the signatory
ITB 23.0	**Deadline for online bid submission:** Time: 05:00 PM Date: 09-01-2023
ITB 26.0	**Timeline for Technical bid Opening:** Time: 03:30 PM Date: 10-01-2023 Venue: O/o AGM (DP&C), TSECL Bidyut Bhawan, Banamalipur, Agartala- 799001, Tripura
ITB 26.0	**Date of Price Bid Opening:** Date and time of price bid opening will be communicated to the technically qualified bidders separately.

Clause	Description
ITB 29.0	1. The price bid will be opened for those bidders who have met the pre-qualification criteria and eligibility as specified in this bid document. 2. The technical Bids along with all the supporting documents shall be submitted in separate folder. Department will review the technical bids of the CSP to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at department's discretion. The CSP's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and technical evaluation framework. Each Technical Bid will be assigned a technical score out of a maximum of 100 marks. Only the bidders who get an aggregate technical score of 70% or more will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid and Bidder.
ITB 36.1	The Contract Performance Guarantee (CPG) shall remain valid for entire contract duration i.e 45(forty-five) months plus 3 (three) months grace period.

4. General Conditions of Contract (GCC)

1.0 Definitions

1.1. 'The Contract' means the agreement entered into between Tripura State Electricity Corporation Limited and Contractor as per the Contract Agreement signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

1.2. 'Owner' or 'Purchaser' shall mean TRIPURA STATE ELECTRICITY CORPORATION LIMITED (TSECL) and shall include their legal representatives, successors and assigns.

1.3. 'Contractor' or 'Supplier' or 'Implementation Partner' shall mean the Bidder whose bid shall be accepted by TSECL for award of the Works/supply and shall include such successful Bidder's legal representatives, successors and permitted assigns.

1.4. 'Sub-contractor' shall mean the person named in the Contract for any part of the Works or any person to whom any part of the Contract has been sublet by the Contractor with the consent in writing of the owner's Engineer in charge of the work and shall include the legal representatives, successors and permitted assigns of such person.

1.5. "ERP" means Enterprise Resource Planning suite as per the requirements of RFP,

1.6. 'Works' shall mean and include furnishing of software, licenses and/or manpower as per the Specifications of Bid Documents and complete implementation services, testing and putting into satisfactory operation including supply, installation, configuration and integration of ERP at the Sites as defined in the Contract/ Bid Document.

1.7. 'Specifications' shall mean the Specifications and Bidding Documents forming a part of the Contract and such other schedules as may be mutually agreed upon.

1.8. 'Site' shall mean and include the offices under TSECL where the services are required to be provided.

1.9. The term 'Contract Price' shall mean the item wise price / lump-sum price quoted by the Contractor in his bid with additions and/or deletions as may be agreed and incorporated in the Letter of Award, for the entire scope of the works.

1.10. 'Manufacturer's Works' or 'Contractor's Works', shall mean the place of work used by the manufacturer, the Contractor, their collaborators/associate or sub-contractors for the performance of the Contract.

1.11. 'Inspector' shall mean TSECL or any person nominated by TSECL from time to time, to inspect the equipment; stores or Works under the Contract and/or the duly authorized representative of TSECL.

1.12. 'Notification of Award of Contract'/Letter of Award'/Telex of Award' shall mean the official notice issued by TSECL notifying the Contractor that his bid has been accepted.

1.13. 'Date of Contract' shall mean the date on which Notification of Award of Contract/Letter of Award/Telex of Award has been issued.

1.14. 'Month' shall mean the calendar month. 'Day or 'Days', unless herein otherwise expressly defined, shall mean calendar day or days of 24 hours each.

1.15. A 'Week' shall mean continuous period of seven (7) days.

1.16. "Writing" shall include any manuscript, type written or printed statement, under or over signature and/or seal as the case may be.

1.17. When the words 'Approved'. Subject to Approval', 'Satisfactory', 'Equal to', 'Proper', 'Requested', 'As Directed', 'Where Directed', 'When 'Determined by', 'Accepted',

'Permitted', or words and phrases of like importance are used, the approval, judgment, direction etc. is understood to be a function of TSECL.

1.18. "Testing during Implementation"/ "Test on Completion" shall mean such tests as prescribed in the Contract/ Bid Document to be performed by the Contractor before the work is Taken Over by TSECL.

1.19. "Initial Operation" shall mean the first integral operation of the complete equipment covered under the Contract with the sub-system and supporting equipment in service or available for service.

1.20. 'Performance and Guarantee Test' shall mean all operational checks and tests required to determine and demonstrate capacity, efficiency and operating characteristics as specified in the Contract Documents.

1.21. The term 'Final Acceptance / Taking Over' shall mean written acceptance of the Works performed under the Contract by TSECL, after successful commissioning/completion of Performance and Guarantee Tests, as specified in the accompanying Technical Specification or otherwise agreed in the Contract.

1.22. "Commercial Operation" shall mean the Conditions of Operation in which the complete equipment covered under the Contract is officially declared by TSECL to be available for continuous operation at different loads up to and including rated capacity. Such declaration by TSECL, however, shall not relieve or prejudice the Contractor of any of his obligations under the Contract.

1.23. 'Guarantee period'/'Maintenance Period' shall mean the period during which the Contractor shall remain liable for repair or replacement of any defective part of the works performed under the contract.

1.24. 'Latent Defects' shall mean such defects caused by faulty designs, material or work man ship which cannot be detected during inspection, testing etc, based on the technology available for carrying out such tests.

1.25. Words imparting 'Person' shall include firms, companies, corporation and association or bodies of individuals.

1.26. Terms and expressions not herein defined shall have the same meaning as are assigned to them in the Indian Sale of Goods Act (1930), failing that in the Indian Contact Act (1872) and failing that in the General Clauses Act (1897) including amendments thereof if any.

1.27. 'Stabilization Period' means successful running of full systems for a period of at least three months from final Go-live declaration by TSECL at all its offices.

1.28. 'Go-live' means the stage where the ERP Solution is available to all the authorized users for executing live transactions to successfully carryout identified functions/processes.

1.29. 'OEM' means Original Equipment Manufacturer of the ERP/software/database/product as per standard practice who are providing such software to the Owner under the scope of this tender/contract.

1.30. 'Bill of Quantity (BoQ)/ Price Schedule' means the rate quoting sheet that must be duly filled by the bidder carefully. It mentions the list of supplies along with the quoted price for each supply and total cost.

1.31. 'Contract Period/Timeline' is the time period for the engagement of Implementation Partner from the date of signing of the Agreement during which the IP is bound by the obligations of this contract.

1.32. 'Representative' means any person nominated by the Implementation Partner and named as such in the contract agreement and approved by TSECL to perform the duties delegated by TSECL.

1.33. 'Scheduled bank' means those banks in India which have been included in the Second Schedule of Reserve Bank of India (RBI) Act, 1934.

1.34. 'Offices' shall mean the Corporate Office, divisional offices, sub-division offices or any other office under TSECL.

1.35. 'Third Party' means any person, firm, company, organization, other than owner

1.36. ''Letter of Authorization' means the license provided by the OEM ERP vendor to the bidder authorizing the use of its products.

1.37. 'Warranty Period' means the period of validity of the warranties given by the Bidder commencing the date of Stabilization Acceptance, during which the Contractor is responsible for defects with respect to the System

1.38. In addition to the above the following definitions shall also apply.

a. 'All software and licenses' to be supplied shall also mean 'Goods'.

b. 'Contract Performance Guarantee shall also mean 'Contact Performance Security'

2.0 Application

These General Conditions shall apply to the extent that they are not **superseded by provisions in other parts of the Contract.**

3.0 Standards

The Goods supplied under this Contract shall conform to the standards mentioned in the Various Technical Specifications and when no applicable standard is mentioned to the authoritative standard appropriate to the Goods and such standards shall be the latest issued by the concerned institution.

4.0 Language and Measures

All documents pertaining to the Contract including specification, Schedules, notices, correspondence, operating and maintenance instructions, drawings or any other writing shall be written in English language. The Metric System of measurement shall be used exclusively in the Contract.

5.0 Contract Documents

The term "Contract Documents" shall mean and include the following which shall be deemed to form an integral part of the Contract:

1. Invitation of Bid including letter forwarding the Bidding Documents, Instructions to Bidders, General Terms and Conditions of Contract and all other documents included under the Special Conditions of Contract and various other sections.
2. Specifications of the equipment to be furnished under the Contract as brought out in the accompanying Technical Specification.
3. Contractor's Bid proposal and the documents attached there-to including the letter of clarifications thereto between the supplier/Contractor and TSECL prior to the Award of Contract.
4. All the materials, literature, data and information of any sort given by the Supplier/Contractor along with his bid, subject to the approval of TSECL.

5. Letter of Award and any agreed variations of the conditions of the documents and special terms and conditions of contract if any.

6.0 Use of the Contract Documents and Information

The Supplier/Contractor shall not communicate or use in advertising, publicity, sales releases or in any other medium, photographs or other reproduction of the Supply under this contract, or descriptions of the site, dimensions, quantity, quality, or other information, concerning the Works unless prior written permission has been obtained from TSECL.

7.0 Jurisdiction of Contract

The laws applicable to the Contract shall be the laws in force in India. The Courts of **Agartala** shall have exclusive jurisdiction in all matters arising **under this Contract.**

8.0 Manner of Execution of Contract

1. The supplier/ contractor should attend the concerned office of TSECL within 15 (fifteen) days from the date of issue of the Letter of Award to the Contractor for signing the contract agreement.
   The Supplier/Contractor shall provide for signing of the Contract, Performance Guarantee, appropriate power of attorney and other requisite materials.
2. The Agreement shall be signed in two originals and the Contractor/supplier shall be provided with one signed original and the rest shall be retained by TSECL.
3. The Supplier/Contractor shall provide free of cost to TSECL all the engineering data, drawings, and descriptive materials submitted with the Bid, in at least six (6) copies to form a part of the contract immediately after issue of Letter of Award.
4. Subsequent to signing of the Contract, the Contractor/supplier, at his own cost, shall provide TSECL with at least six (6) true copies of Agreement and one soft copy.

9.0 Assistance

The TSECL will ensure, through its Project Co-Ordinator, transfer of information, specification of mutually agreed change-requirements (Change Requests), meetings with relevant users and other personnel.

10.0 Methodology, Tools and Techniques

Bidder will use the methodology, tools and techniques as stated in the accompanying Technical Proposal. Any change in these, if desired by the TSECL will need to be communicated to Bidder in writing with a reasonable notice period to allow for an assessment of their impact, if any, on schedule, technical requirements, feasibility and cost.

11.0 Deliverables

The deliverables will be as per the details of the deliverables provided in the accompanying Technical Proposal.

12.0 Acceptance of Deliverables

TSECL will carry out acceptance of deliverables as per the schedule presented in the accompanying Technical Proposal.

The application software (if any) will be delivered/installed for acceptance to TSECL as and when the same is ready for delivery. The actual Acceptance Testing of the software will be the responsibility of TSECL. TSECL will prepare the Acceptance Test data along with the expected test results (consistent with the detailed specifications of the system and any

change-request agreed in the documents) and keep it ready at least four (4) weeks in advance before the scheduled commencement of the Acceptance Testing of the software. The acceptance testing will be based on the test cases provided by TSECL. Bidder will provide support for any clarifications during the Acceptance Testing of the system. Defects if any, observed by TSECL, will be notified to Bidder in writing within two (2) weeks of delivery. Bidder will correct the defects and subsequently TSECL will confirm acceptance in writing to Bidder. The TSECL shall not withhold or delay the issuance of acceptance certificate of any of the deliverables, if the deliverables substantially meet the specifications or on account of any minor defects which have no material effect on the functionality of the deliverables.

Reworking of defects shall be at the cost of Bidder provided the defects are for reasons solely and entirely attributable to the Bidder. Items reported as defects that are not deviations from the immediate previous accepted baseline will be reported again through fresh Change Request documents under the Change Management Procedure described herein. Items reported through the Change Management Procedure will be dealt with separately.

13.0 Change Management Procedure

A change identified at any stage of the assignment which requires the deliverable to deviate from the then current baseline or the approved deliverable of the previous baseline to be modified, will be conveyed by the TSECL to Bidder or vice-versa in the form of a Change Request document. The request for change will then be assessed by Bidder to evaluate its impact on feasibility, time schedules, technical requirements in consequence of the proposed change and cost. Bidder will present this assessment to the TSECL for its approval within a reasonable time period. Bidder will incorporate the change after receiving the TSECL's written approval.

14.0 Enforcement of Terms

The failure of either party to enforce at any time any of the provisions of this Contract or any rights in respect thereto or to exercise any option therein provided, shall in no way be construed to be a waiver of such provisions, rights or options or in any way to affect the validity of the Contract. The exercise by either party of any of its rights herein shall not prejudice either party from exercising the same or any other right it may have under the **Contract**.

15.0 Completion of Contract

Unless otherwise terminated under the provisions of any other relevant clause, this Contract shall be deemed to have been completed on the date stipulated in the NIT.

16.0 Time – The essence of Contract

16.1. The time and the date of completion of the Contract as stipulated in the Contract by TSECL without or with modifications, if any, and so incorporated in the Letter of Award, shall be deemed to be the essence of the Contract. The Contractor/supplier shall so organize his resources and perform his Work as to complete it not later than the date agreed to.

16.2. The Contractor/supplier shall submit a detailed BAR CHART / PERT NETWORK consisting of adequate number of activities covering various key phases of the Work as mentioned in Section 6 Scope of Work within fifteen (15) days of the date of Notice of Award of Contract. This Bar Chart shall also indicate the interface facilities to be provided by TSECL and the dates by which such facilities are needed. The supplier/ Contractor shall discuss with TSECL for finalization and approval of the Bar Chart by TSECL. The agreed Bar Chart shall form part of the contract documents. During the performance of the Contract, if in the opinion of the owner's Engineer in charge of the work, proper progress is not maintained, suitable changes shall be made in the Supplier/Contractor's operations to ensure proper progress without any cost implication to TSECL. The interface facilities to be provided by TSECL in accordance with the agreed Bar Chart shall also be reviewed while reviewing the progress of the Contractor.

16.3. Based on the agreed Bar Chart fortnightly reports shall be submitted by the Contractor as directed by the owner's Engineer in charge of the work.

16.4. Subsequent to the finalization of the Bar Chart, the Supplier/Contractor shall make available to the owner's Engineer in charge of the work a detailed manufacturing programme/ Work Plan in line with the agreed Contract Bar Chart. Such manufacturing programme/ Work Plan shall be reviewed, updated and submitted to the owner's Engineer in charge of the work once in every month thereafter.

16.5. The above Bar Charts/manufacturing programme/ Work Plan shall be compatible with TSECL computer environment and furnished to TSECL on such media as may be desired by TSECL.

17.0 Effectiveness of Contract

The Contract shall be considered as having come into force from the date of the Notification of Award, unless otherwise provided in the Notification of Award.

18.0 Extension of Time

18.1. The TSECL may consider to grant extension of time for the completion of the work if it is felt absolutely essential on fulfillment of following conditions by the contractors and on reasons which would be beyond the control of the bidder: -

a. The supplier/contractor must apply to the Engineer-in-charge in writing for extension of time in writing so required justifying the necessity.
b. Such application must state the grounds which hindered the supply/contractor in the execution of the work within the time as stipulated in the contract document/ agreement.
c. Such application must be made within 30 days of the date on which such hindrance had arisen.
d. The Engineer-in-charge must be of the opinion that the grounds shown for the extension of time are reasonable and without extension of such time completion of the work is practically impossible.

18.2. According to the terms of the contract the Engineer- in -charge has full powers, but the orders on the application of the supplier/ contractor connected with the agreement accepted by the authorities higher than the Engineer-in-charge should be issued by him only after written approval of the authorities higher than the Engineer-in-charge.

18.3. The opinion of the Engineer-in-charge, whether the grounds shown for the extension of time are or are not reasonable, is final. If the Engineer-in-charge is of the opinion that the Grounds shown by the supplier/ contractor are not reasonable and declines to the grant extension to time, the supplier/contractor cannot challenge.

19.0 Liquidated Damages

In case the materials are not delivered within the time stipulated in the order or delay in achieving the milestones defined under Section 6 Scope of Work or in case of un-performed services, the supplier shall have to pay at the discretion of the competent authority of purchaser, the liquidated damages to be determined by the purchaser as 1 % of the delivered price of the delayed goods or un-performed services for each week of delay until actual delivery or performance subject to a maximum deduction of 10% of the delayed goods/services price. Due consideration may be given in the levy of damages for reasons absolutely beyond the control of the supplier for which documentary evidence shall be provided to the satisfaction of the competent delayed supplies

20.0 Taxes, Permits & Licenses

The Supplier/Contractor shall pay all non-Indian taxes, duties, levies lawfully assessed against TSECL or the Contractor in pursuance of the Contract. In addition, the Contractor shall be responsible for payment of all Indian duties, levies and taxes lawfully assessed against this contract.

21.0 Deduction

Any amount which becomes payable by the supplier under particular contract shall be deducted by the purchaser from any amount that is due or becoming due under the same or any other contract and shall be adjusted.

22.0 Limitation of Liabilities

The final payment by TSECL in pursuance of the Contract shall mean the release of the Contractor from all his liabilities under the Contract. Such final payment shall be made only at the end of the Guarantee/Warranty Period, and till such time as the contractual liabilities and responsibilities of the Contractor, shall prevail. All other payments made under the Contract shall be treated as on-account payments.

23.0 Change of Quantity

23.1. During the execution of the Contract, TSECL reserves the right to increase or decrease the quantities of items under the Contract but without any change in unit price or other terms & conditions. Such variations shall not be subjected to any limitation for the individual items **but the total variations in all such items under the Contract shall be limited to ±25% of the contract value.**

23.2. The Contract price shall accordingly be adjusted based on the unit rates available in the Contract for the change in quantities as above. The base unit rates, as identified in the Contract shall however remain constant during the currency of the Contract, except as provided for in clause 33.0 below. In case, the unit rates are not available for the change in quantity, the same shall be subjected to mutual agreement.

24.0 No Waiver Rights of Agreement/Contract Provision

Neither the inspection by TSECL nor any order by TSECL for payment of money or any payment for or acceptance of, the whole or any part of the supply by the Engineer in charge of the supply, nor any possession taken by the Engineer in charge of the supply shall operate as a waiver of any provision of the Contract, or of any power herein reserved to Engineer or any right to damages herein provided nor shall any waiver of any breach in the Contract be held to be a waiver of any other or subsequent breach.

25.0 Certificate not to affect Right of TSECL and Liability of Contractor.

No interim payment certificate of the owner's Engineer in charge of the work, nor any sum paid on account by TSECL, nor any extension of time for execution of the Works granted by TSECL shall affect or prejudice the rights of TSECL against the Contractor or relieve the Contractor of his obligation for the due performance of the Contractor, or be interpreted as approval of the Works done or of the equipment furnished and no certificate shall create liability for TSECL to pay for alterations, amendments, variations or additional works not ordered, in writing, by the owner's Engineer in charge of the work or discharge the liability of the Contractor for the payment of damages whether due, ascertained or certified or not or any sum against the payment of which he is bound to indemnify TSECL, nor shall any such certificate nor the acceptance by him of any sum paid on account or otherwise affect or prejudice the rights of TSECL against the Contractor.

26.0 Contract Performance Guarantee

The Contractor shall furnish Contract Performance Guarantee as specified in Section - I & Section-II for the proper fulfillment of the Contract within Fifteen (15) days of "Notice of Award of Contract."

27.0 Contract Price Adjustment

All prices / price components of the contract shall remain firm and no adjustment of price, whatsoever, shall be applicable during the currency of contract.

28.0 Payment

1. For tenderer(s) payment will be made through RTGS within 60 (sixty days) of submission of invoice in complete shape along with required documents / certificates.
2. Payment will be made in accordance with Payment Schedule in Section 5 Special Condition of Contract.
3. Any terms of advance payments i.e. payments against dispatch documents/Bank documents will not be acceptable.
4. In no circumstances, claim of interest on payment shall be entertained.

28.1. Payment Terms

i. Operational Expenditure (Opex) will be paid on Quarterly basis after submission of relevant report/documents as per service. **The first quarter shall begin from date of Setup Go Live.**

ii. Quarterly payment against Item of Agreement along with GST will be calculated based on usage of services (equivalent vCPUs, RAM and storage space, etc. as per mentioned in Price Bid) provided by bidder. This quarterly payment will be arranged on or after 30 days from date of completion of each quarter on satisfactory provision of cloud services by the bidder and on production of invoice.

iii. Total Quarterly Payment should be linked to the compliance with the SLA metrics and the actual payment is the payment due to the Service Provider after any SLA related deductions.
iv. Deployment plan will be shared with successful bidder post kick off meeting.
v. The bidder shall submit the RTGS details (i.e. IFSC code, Bank Account No., Name & Branch of Bank) along with PAN/TIN & GST number details in the 1st running bill and also submit the proof of GST registration to TSECL.
vi. All payment shall be made subject to deduction of TDS as per the Income tax act and/or any other statutory provisions

28.2. Currency of Payment

All payments under the Contract shall be in Indian Rupees only.

28.3. Due Dates for Payments

TSECL will make progressive payment as and when the payment is due as per the terms of payment set forth as herein after.

29.0 Mode of Payment

Payment due on supply materials / services shall be made by the owner's Engineer in charge of the work through RTGS.

30.0 Insurance

30.1. The Contractor at his cost shall arrange, secure and maintain all insurance as may be pertinent to the Works and obligatory in terms of law to protect his interest and interests of TSECL against all perils detailed herein. The form and the limit of such insurance as defined herein together with the under-writer in each case shall be acceptable to TSECL. However, irrespective of such acceptance, the responsibility to maintain adequate insurance coverage at all times during the period of Contract shall be of the Contractor alone. The Contractor's failure in this regard shall not relieve him of any of his contractual responsibilities and obligations. The insurance covers to be taken by the Contractor shall be in a joint name of TSECL and the Contractor. The Contractor shall, however, be authorized to deal directly with Insurance Company or Companies and shall be responsible in regard to maintenance of all insurance covers. Further the insurance should be in freely convertible currency.

30.2. Any loss or damage to the equipment during handling, transportation, storage, installation, putting into satisfactory operation and all activities to be performed till the successful completion of commissioning of the equipment shall be to the account of the Contractor. The Contractor shall be responsible for preference of all claims and make good the damages or loss by way of repairs and/or replacement of the equipment, damaged or lost. The transfer of title shall not in any way relieve the Contractor of the above responsibilities during the period of Contract. The Contractor shall provide TSECL with copy of all insurance policies and documents taken out by him in pursuance of the Contract. Such copies of documents shall be submitted to TSECL immediately after such insurance coverage. The Contractor shall also inform TSECL in writing at least Sixty (60) Days in advance regarding the expiry/cancellation and/or change in any of such documents and ensure revalidation, renewal etc., as may be necessary well in time.

30.3. The perils required to be covered under the insurance shall include, but not be limited to fire and allied risks, miscellaneous accidents (installation risks) workman compensation risks,

loss or damage in transit, theft, pilferage, riot, strikes, social unrest and malicious damages, civil commotion, weather conditions, accidents of all kinds, etc. The scope of such insurance shall be adequate to cover the replacement/reinstatement cost of the equipment for all risks upto and including delivery of goods and other costs till the goods are delivered at Site. The insurance policies to be taken should be on replacement value basis and/or incorporating escalation clause. Notwithstanding the extent of insurance cover and the amount of claim available from the underwriters, the Contractor shall replace/rectify full quantities of all equipment /materials in good condition and to ensure their availability as per project requirements.

30.4. All costs on account of insurance liabilities covered under the Contract will be to Contractor's account and will be included in Contract Price, However, TSECL may from time to time, during the pendency of the Contract, ask the Contractor in writing to limit the insurance coverage, risks and in such a case, the parties to the Contract will agree for a mutual settlement, for reduction in Contract price to the extent of reduced premium amount. The Contractor, while arranging the insurance shall ensure to obtain all discounts on premium, which may be available for higher volume or for reason of financing arrangement of the project.

31.0 Liability

Bidder shall be excused and not be liable or responsible for any delay or failure to perform the services or failure of the services or a deliverable under this Agreement, to the extent that such delay or failure has arisen as a result of any delay or failure by the TSECL or its employees or agents or third-party service providers to perform any of its duties and obligations as set out in this Agreement. In the event that Bidder is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of the TSECL, then Bidder shall be allowed an additional period of time to perform its obligations and unless otherwise agreed the additional period shall be equal to the amount of time for which Bidder is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of the TSECL. Such failures or delays shall be brought to the notice of the TSECL and subject to mutual agreement with the TSECL, then Bidder shall take such actions as may be necessary to correct or remedy the failures or delays. Bidder shall be entitled to invoice the TSECL for additional costs incurred in connection with correction or remedy as above at time & material rate card as agreed upon between the parties.

Neither party shall be liable to the other for any special, indirect, incidental, consequential (including loss of profit or revenue), exemplary or punitive damages whether in contract, tort or other theories of law, even if such party has been advised of the possibility of such damages.

The total cumulative liability of either party arising from or relating to this Agreement shall not exceed the total amount paid to Bidder by the TSECL in the preceding twelve months under that applicable work that gives rise to such liability (as of the date the liability arose).

32.0 Liability for accidents and damages

Under the Contract, the Contractor/ Supplier shall be responsible for loss or damage to the equipment until the successful completion of commissioning as defined else-where in the Bidding Documents.

In case of a default on bidder's part or other liability, TSECL shall be entitled to recover damages from the Contractor. In each such instance, regardless of the basis on which TSECL is entitled to claim damages from the Contractor (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), Contractor shall be liable for no more than:

1. Payment referred to in the Patents and Copyrights clause.
2. Liability for bodily injury (including death) or damage to real property and tangible personal property limited to that cause by the Contractor's negligence.
3. As to any other actual damage arising in any situation involving nonperformance by Contractor pursuant to or in any way related to the subject of this Agreement, the charge paid by TSECL for the individual product or Service that is the subject of the Claim. However, the contractor shall not be liable for
4. For any indirect, consequential loss or damage, lost profits, third party loss or damage to property or loss of or damage to data.
5. For any direct loss or damage that exceeds the total payment for Contract Price made or expected to be made to the Contractor hereunder.
6. Subject to the above, the aggregate liability of the Consultant, under this Contract, regardless of the form of claim shall not exceed 100% of the contract value.

33.0 General Indemnity

The TSECL will, during the period of the coverage of this assignment, indemnify and hold Bidder harmless from any loss, injury, claim or damage resulting from any death or injury to any person or property of Bidder arising out of the use or possession of the equipment or location of the TSECL by Bidder or its personnel, unless caused by the negligence of Bidder personnel and the limitation or liability provided herein shall not apply to such loss, injury, claim or damages.

34.0 Intellectual Property Rights

1. The Bidder hereby represents and warrants that:

   (a) the goods and services as supplied, installed, tested, and accepted;
   (b) use of the goods and services in accordance with the Contract; and
   (c) copying of the goods and services provided to the Purchaser in accordance with the Contract

TSECL does not and will not infringe any Intellectual Property Rights held by any third party and that it has all necessary rights or at its sole expense shall have secured in writing all transfers of rights and other consents necessary to make the assignments, licenses, and other transfers of Intellectual Property Rights and the warranties set forth in the Contract, and for the Purchaser to own or exercise all Intellectual Property Rights as provided in the Contract. Without limitation, the Bidder shall secure all necessary written agreements, consents, and transfers of rights from its employees and other persons or entities whose services are used for development of the System.

All intellectual property rights in the software, all tools, processes, software, utilities and methodology including any Bidder proprietary products or components thereof any development carried out by Bidder thereto in the course of providing services hereunder, including customization, enhancement, interface development etc. shall remain the exclusive property of Bidder and the TSECL shall not acquire any right title or interest of any nature therein except to the extent provided herein.

Bidder 's Proprietary Software and Pre-Existing IP:- TSECL acknowledges and agrees that this is a professional services agreement and this agreement is not intended to be used for licensing of any Bidder 's proprietary software or tools. If Supplier and TSECL mutually agree that the Bidder provides to TSECL any proprietary software or tools of Bidder or of a third party, the parties shall negotiate and set forth the applicable terms and conditions in a separate license agreement and the provisions of this Clause shall not apply to any deliverables related to customization or implementation of any such proprietary software or products of Bidder or of a third party. Further, TSECL acknowledges that in performing Services under this Agreement Bidder may use Bidder 's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by Bidder prior to or independent of the Services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the Services hereunder, ("Bidder Pre-Existing IP"). Notwithstanding anything to the contrary contained in this Agreement, Supplier shall continue to retain all the ownership, the rights title and interests to all Bidder Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting Bidder from using Supplier Pre-Existing IP in any manner. To the extent that any Bidder Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under this Agreement, Supplier hereby grants to TSECL a non-exclusive, perpetual, royalty free, fully paid up, irrevocable license, with the right to sublicense through multiple tiers, to use, copy, install, perform, display, modify and create derivative works of any such Bidder Pre-Existing IP in connection with the deliverables and only as part of the Deliverables in which they are incorporated or embedded. The foregoing license does not authorizes TSECL to (a) separate Bidder Pre-Existing IP from the deliverable in which they are incorporated for creating a stand-alone product for marketing to others; (b) independently sell, lease, exchange, mortgage, pledge, license, sub license, assign or in any other way convey, transfer or alienate the Bidder Pre-Existing IP in favour of any person (either for commercial consideration or not (including by way of transmission), and/or (c) except as specifically and to the extent permitted by the Supplier in the relevant Statement of Work, reverse compile or in any other way arrive at or attempt to arrive at the source code of the Bidder Pre-Existing IP.

35.0 Intellectual Property Rights Indemnity

1. The Bidder shall indemnify and hold harmless the Purchaser and its employees and officers from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability), that the Purchaser or its

employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights by reason of:

(a) Installation of the System by the Bidder or the use of the System, including the Materials, in the country where the site is located;
(b) Copying of the Software and Materials provided the Bidder in accordance with the Agreement; and
(c) sale of the products produced by the System in any country, except to the extent that such losses, liabilities, and costs arise as a result of the Purchaser's breach of GCC Clause 28 (2)

2. Such indemnity shall not cover any use of the System, including the Materials, other than for the purpose indicated by or to be reasonably inferred from the Contract, any infringement resulting from the use of the System, or any products of the System produced thereby in association or combination with any other goods or services not supplied by the Bidder, where the infringement arises because of such association or combination and not because of use of the System in its own right.
3. Such indemnities shall also not apply if any claim of infringement:
   (a) Is asserted by a parent, subsidiary, or affiliate of the Purchaser's organization;
   (b) is a direct result of a design mandated by the Purchaser's Technical Requirements and the possibility of such infringement was duly noted in the Bidder's Proposal; or
   (c) results from the alteration of the System, including the Materials, by the Purchaser or any persons other than the Bidder or a person authorized by the Bidder.
4. If any proceedings are brought or any claim is made against the Purchaser arising out of the matters referred to in GCC Clause 29 (1), the Purchaser shall promptly give the Bidder notice of such proceedings or claims, and the Bidder may at its own expense and in the Purchaser's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim.
5. If the Bidder fails to notify the Purchaser within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its own behalf. Unless the Bidder has so failed to notify the Purchaser within the twenty-eight (28) days, the Purchaser shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Purchaser shall, at the Bidder's request, afford all available assistance to the Bidder in conducting such proceedings or claim and shall be reimbursed by the Bidder for all reasonable expenses incurred in so doing.
6. The Purchaser shall indemnify and hold harmless the Bidder and its employees, officers, and Subcontractors from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Bidder or its employees, officers, or Subcontractors may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights arising out of or in connection with any design, data, drawing, specification, or other documents or materials provided to the Bidder in connection with this Contract by the Purchaser or any persons (other than the Bidder) contracted by the Purchaser, except to the extent that such losses, liabilities, and costs arise as a result of the Bidder's breach of GCC Clause 29 (8).

7. Such indemnity shall not cover

(a) any use of the design, data, drawing, specification, or other documents or materials, other than for the purpose indicated by or to be reasonably inferred from the Contract;

(b) any infringement resulting from the use of the design, data, drawing, specification, or other documents or materials, or any products produced thereby, in association or combination with any other Goods or Services not provided by the Purchaser or any other person contracted by the Purchaser, where the infringement arises because of such association or combination and not because of the use of the design, data, drawing, specification, or other documents or materials in its own right.

8. Such indemnities shall also not apply:

(a) if any claim of infringement is asserted by a parent, subsidiary, or affiliate of the Bidder's organization;

(b) to the extent that any claim of infringement is caused by the alteration, by the Bidder, or any persons contracted by the Bidder, of the design, data, drawing, specification, or other documents or materials provided to the Bidder by the Purchaser or any persons contracted by the Purchaser.

9. If any proceedings are brought or any claim is made against the Bidder arising out of the matters referred to in GCC Clause 29 (5), the Bidder shall promptly give the Purchaser notice of such proceedings or claims, and the Purchaser may at its own expense and in the Bidder's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Purchaser fails to notify the Bidder within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Bidder shall be free to conduct the same on its own behalf. Unless the Purchaser has so failed to notify the Bidder within the twenty-eight (28) days, the Bidder shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Bidder shall, at the Purchaser's request, afford all available assistance to the Purchaser in conducting such proceedings or claim and shall be reimbursed by the Purchaser for all reasonable expenses incurred in so doing.

36.0 Residuary Rights

Each Party shall be entitled to use in the normal course of its business and in providing same or similar services or development of similar deliverables for its other clients, the general knowledge and experience gained and retained in the unaided human memory of its personnel in the performance of this Agreement and Statement of Work(s) hereunder. For the purposes of clarity, the Supplier shall be free to provide any services or design any deliverable(s) that perform functions same or similar to the deliverables being provided hereunder for the Client, for any other customer of the Supplier (including without limitation any affiliate, competitor or potential competitor of the TSECL). Nothing contained in this Clause shall relieve either party of its confidentiality obligations with respect to the proprietary and confidential information or material of the other party

Similarly, all the Intellectual Property Rights (IPR) in the third-party software used in providing services including those forming part of or incorporated into the deliverables

shall remain with the respective third-party owners/ Bidder's licensor and TSECL shall have user rights in accordance with end user license agreement (EULA) as applicable to use of such software.

37.0 Additional Support and Services

In case the TSECL requires any additional support in execution of its tasks in respect of the assignment, it shall be provided to them by Bidder on change request basis.

38.0 Confidentiality

Both parties agree that they may, in the course of their business relationship with the other, acquire or be exposed to information that is proprietary or confidential to the other party, its affiliates or its or their respective clients. Both parties undertake, to hold all such information in strictest confidence and not to disclose such information to third parties nor to use such information for any purpose whatsoever save as may be strictly necessary for the performance of the assignment as mentioned in this proposal. The term "Confidential Information" as used herein means any information or documents disclosed by one party to the other party orally, and which is reduced to writing within a period of 3 days of the disclosure or in writing or including but not limited to any written or printed documents, samples, model, technical data/know-how, drawings, photographs, specifications, standards, manuals, reports, formulae, algorithms, processes, information, lists, trade secrets, computer programs, computer software, computer data bases, computer software documentation, quotations and price lists, research products, inventions, development, processes, engineering techniques, strategies, customers, internal procedures, employees and business opportunity and clearly identified and marked as "Confidential Information". The data contained herein shall not be disclosed, duplicated, used in whole or in part for any purpose other than to evaluate the proposal provided that, a contract is awarded to this proposal as a result of, or in connection with the submission of this data. Both the parties shall have the right to duplicate, use or disclose the data to the extent provided in the contract. This confidentiality restrictions shall be for the term of the resultant contract and for a period of two years thereafter. This restriction does not limit the right to use information contained in the data if it:

a. Is obtained from another source without restriction.
b. Is in the possession of, or was known to, the receiving party prior to its receipt, without an obligation to maintain confidentiality,
c. becomes generally known to the public without violation of this Proposal,
d. is independently developed by the receiving party without the use of confidential Information and without the participation of individuals who have had access to confidential information,
e. is required to be provided under any law, or process of law duly executed.

39.0 Non-employment

The TSECL will neither offer to employ nor employ, directly or otherwise, any Bidder employee, associated for the purpose of, or with the assignment, during the period between the date of this proposal and two years from the completion of the assignment arising here from.

40.0 Waiver

No forbearance, indulgence or relaxation by any Party at any time to require performance of any provision of this Proposal shall in any way affect, diminish or prejudice the right of such party to require performance of that provision and any waiver by any party or any breach of any provisions of this Proposal shall not be construed as a waiver or an amendment of the provisions itself, or a waiver of any right under or arising out of this Proposal.

41.0 Assignment

Neither Party shall be entitled to assign or transfer all or any of its rights, benefits and obligations under this proposal without the prior written consent of the other Party.

42.0 Nonexclusively

Bidder shall be free to do similar business either for itself or for any other party or offer similar services to any third parties but without in any way affecting the services agreed to be offered by Bidder under this Proposal.

43.0 Independent Relationship

This RFP is not intended to create a relationship such as a partnership, joint venture, agency, or employment relationship. Neither party may act in a manner, which expresses or implies a relationship other than that of independent party nor bind the other party.

44.0 Interpretation

In the event of a dispute between the parties, this Agreement will not be construed for or against either party but will be interpreted in a manner consistent with the intent of the parties as evidenced by the terms of this Agreement. Unless otherwise specified, "days" means calendar days.

45.0 Publicity

Neither party shall publicize any information pertaining to this assignment or the other party without seeking the prior written consent of the other party.

46.0 Entire Understanding

This Proposal together with the Schedules, Annexure and Exhibits hereto and executed by the parties hereto constitutes the entire understanding between the parties hereto with respect to the subject matter hereto and supercedes and cancels all previous negotiations thereof. To the extent permitted by Applicable Law, a party is not liable to another party in contract or tort or in any other way for a representation or warranty that is not set out in this Agreement.

47.0 Survival

The clauses of this proposal which by their nature are intended to survive shall so survive the termination/expiry of this proposal.

48.0 Demurrage, wharfage, etc.

All demurrage, wharf age and other expenses incurred due to delayed clearance of the material or any other reason shall be to the account of the Contractor/Supplier.

49.0 Force Majeure

Except to the extent otherwise provided herein, no liability shall result to other Party from delay in performance of from non-performance caused by circumstances beyond the control of the Party affected, including but not limited to act of God, fire, flood, explosion, war, action or request of governmental authority, accident, labour trouble but each of the hereto shall be diligent in attempting to remove such cause or causes. In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If such an event lasts for a continuous period of thirty (30) days, then either party may at any time thereafter while such performance continues to be excused, terminate this Assignment without liability, by notice in writing to the other party. However, Bidder shall be entitled to receive payments for all services rendered by it under this Assignment.

Any delay or hinderance in delivery by Bidder as a result of the occurrence of any Force Majeure Event to its suppliers or subcontractors shall be deemed as a Force Majeure Event occurring to Bidder.

50.0 Contractor's Default

50.1. The Supplier/Contractor shall have to pay liquidated damages for delay in completion of Works as defined in "Liquidated Damages" of this Section.

The termination of the Contract under this clause shall neither entitle the Contractor to reduce the value of the Contract Performance Guarantee nor the time thereof. The Contract Performance Guarantee shall be valid for the full value and for the full period of the Contract including guarantee period

51.0 Termination of Contract

The Agreement resulting from this proposal may be terminated:

(a) by either party by giving the other party not less than ninety (90) days written notice of termination,

(b) forthwith if either party commits any material breach of any term of this contract and which in the case of a breach capable of being remedied shall not have been remedied within thirty (30) working days of written notice to remedy the same,

(c) forthwith by either party if the other party shall convene a meeting of its creditors or if a proposal is made for a declaration as insolvent or a proposal for any other composition scheme or arrangement (or assignment for the benefit of its creditors), or if a trustee receiver, administrative receiver or similar officer is appointed in respect of all or any part of the business assets of the other party or if an order is made or a resolution is passed for the purpose of the winding-up of the other party or for the making of an administration order (otherwise than for the purpose of amalgamation or reconstruction),

(d) by either party pursuant to Force Majeure.

Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities of either party nor the coming into force or continuation in force of any provision hereof

which is expressly intended to come into force or continue in force on or after such termination.

In the event of this assignment being terminated, the TSECL shall be liable to make payments of all the amount due under this assignment for which services have been rendered by Bidder's Consultant's. Forthwith on the expiry or earlier termination of this agreement, each party shall, return to the other party all documents and materials, belonging to the other party with regard to this assignment, or shall at the option of the disclosing party destroy all documents or materials in connection with this assignment.

52.0 Grafts and Commissions etc.

Any graft, commission, gift or advantage given, promised or offered by or on behalf of the Contractor or his partner, agent, officers, director, employee or servant or any one on his or their behalf in relation to the obtaining or to the execution of this or any other Contract with the Owner, shall in addition to any criminal liability which it may incur, subject the Contractor to the cancellation of this and all other contracts and also to payment of any loss or damage to the Owner resulting from any cancellation. The Owner shall then be entitled to deduct the amount so payable from any monies otherwise due to Contractor under the Contract.

53.0 Settlement of Disputes

53.1. Any dispute(s) or difference(s) arising out of or in connection with the Contract shall, to the extent possible, be settled amicably between the parties.

53.2. If any dispute or difference of any kind whatsoever shall arise between the Owner and the Contractor, arising out of the Contract for the performance of the Works whether during the progress of the Works or after its completion or whether before or after the termination, abandonment or breach of the Contract, it shall, in the first place, be referred to and settled by the Engineer, who, within a period of thirty (30) days after being requested by either party to do so, shall give written notice of his decision to the Owner and the Contractor.

53.3. Save as hereinafter provided, such decision in respect of every matters so referred shall be final and binding upon the parties until the completion of the Works and shall forthwith be given effect to by the Contractor who shall proceed with the Works with all due diligence, whether he or the Owner requires arbitration as hereinafter provided or not

53.4. If after the Engineer has given written notice of his decision to the parties, no claim to arbitration has been communicated to him by either party within thirty (30) days from the receipt of such notice, the said decision shall become final and binding on the parties.

53.5. In the event of the Engineer failing to notify his decision as aforesaid within thirty (30) days after being requested as aforesaid, or in the event of either the Owner or the Contractor being dissatisfied with any such decision, or within thirty (30) days, after the expiry of the first mentioned period of thirty (30) days, as the case may be, either party may require that the matters in dispute be referred to arbitration as hereinafter provided

54.0 Arbitration

In the event of a dispute or difference of any nature whatsoever between Bidder and the TSECL during the course of the assignment arising as a result of this proposal, the same will

be referred for arbitration to a Board of Arbitration. Such Arbitration shall be governed by the provisions of the Indian Arbitration and Conciliation Act 1996. This Board will be constituted prior to the commencement of the arbitration and will comprise of two arbitrators and an umpire. Bidder and the TSECL will each nominate an arbitrator to the Board and these arbitrators will appoint the umpire. Arbitration will be carried out in Agartala.

55.0 Governing law

This proposal shall be governed by and construed in accordance with Laws of India and the parties submit to the exclusive jurisdiction of the courts in Agartala.

56.0 Owner's Lien on equipment

TSECL shall have a lien on all equipment including those of the Supplier/Contractor brought to the Site for the purpose of installation, testing and commissioning of the equipment, machine(s), other Hardware to be supplied & installed under the Contract. TSECL shall continue to hold the lien on all such equipment throughout the period of Contract. No material brought to the Site shall be removed from the Site by the Supplier/Contractor and/or his Sub-Contractors without the prior written approval of the Engineer.

57.0 Safety Rules

57.1. The following need to be followed:

a. Each employee shall be provided with initial indoctrination regarding safety by the Contractor, so as to enable him to conduct his work in a safe manner.
b. No employee shall be given a new assignment of work unfamiliar to him without proper introduction as to the hazard's incident thereto, both to himself and his fellow employees.
c. Under no circumstances shall an employee hurry or take unnecessary chance when working under hazardous conditions.
d. Employees under the influence of any intoxicating beverage, even to the slightest degree shall not be permitted to remain at work.
e. There shall be a suitable arrangement at every work site for rendering prompt and sufficient first aid to the injured.

57.2. The Contractor shall follow and comply with all relevant Safety Rules, relevant provisions of applicable laws pertaining to the safety of workmen, employees, plant and equipment as may be prescribed from time to time without any demur, protest or contest or reservation. In case of any discrepancy between statutory requirement and relevant Safety Rules referred above, the later shall be binding on the Contractor unless the statutory provisions are more stringent.

57.3. If the Contractor does not take all safety precautions and/or fails to comply with the Safety Rules as prescribed by the Authority or under the applicable law for the safety of the equipment and plant and for the safety of personnel and the Contractor does not prevent hazardous conditions which cause injury to his own employees or employees of other contractors, or Employees of TSECL or any other person who are at Site or adjacent thereto, the Contractors shall be responsible for payment of compensation to the affected persons as per the compensation order issued by the appropriate authority of Government of Tripura / verdict issued by court.

The compensation mentioned above shall be in addition to the compensation payable to the workmen / employees under the relevant provisions of the Workmen's Compensation Act and rules framed there under or any other applicable laws as applicable from time to time. In case TSECL is made to pay such compensation then the amount of such compensation shall be deducted from the progressive bills / contract performance guaranty of the contractor.

58.0 Conflict of Interest

58.1. Bidder shall not engage, and shall cause their Personnel not to engage, either directly or indirectly, in any business or professional activities, which would conflict with the activities assigned to them under this Contract.

58.2. The Purchaser considers a conflict of interest to be a situation in which a party has interests that could improperly influence that party's performance of official duties or responsibilities, contractual obligations, or compliance with applicable laws and regulations, and that such conflict of interest may contribute to or constitute a prohibited corrupt practice.

58.3. If Bidder is found to be involved in a conflict of interest situation with regard to the present assignment, the Purchaser may choose to terminate this contract as per Clause 37.

5. Special Conditions of Contract (SCC)

The following Special Conditions of Contract (SCC) shall supplement the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions herein shall prevail over those in the GCC.

GCC Reference	Description
GCC 1.4	Sub-contracting not allowed except on prior permission of TSECL for some specific exceptional circumstances.
GCC 5.0	Documents relevant for complying with various technical evaluation requirement are also to be a part of Contract Document
GCC 11.0	1. If the Successful Bidder fails to start the Project within the timeline mentioned in Section 15 ITB of the Bid Document, his Bid Security will be forfeited and the Purchaser will have right to cancel the LoA and negotiate with the Bidder having second highest Final Score for placing the fresh LoA or invite fresh Bids.
GCC 11.2	The implementation partner to submit a detailed BAR CHART / PERT NETWORK consisting of adequate number of activities covering various key phases of the Scope of Work as defined in Section 6 to the Project Manager (TSECL) within fifteen (15) days of the date of Notice of Award of Contract.
GCC 13.0	**Causes for Extension of Time for Completion** a. The Supplier/ IP may submit application for an extension of the time for completion if he is or will be delayed in completing the Scope of Work by any of the following causes: i. Additional work ordered in writing; ii. Suspension of work ordered in writing by the Purchaser for no fault on the part of the Supplier/ IP; iii. The delay in completion of Scope of Work caused for no fault on the part of the Supplier/ IP due to orders/ instructions issued by the Purchaser; or iv. Force Majeure as per GCC 30. b. The Supplier/ IP shall give notice to the Purchaser of his intention to make a claim for an extension of time within fifteen (15) calendar days of the occurrence of any of the above cause(s). The notice shall be followed as soon as possible by the claim with full supporting details. c. The Supplier/ IP shall demonstrate to the Purchaser's satisfaction that it has used its best endeavor to avoid or overcome such causes for delay and the Parties will mutually agree upon remedies to mitigate or overcome causes for such delays. d. Notwithstanding the clause above, the Supplier/ IP shall not be entitled to an extension of time for completion, unless the Supplier/ IP, at the time of such circumstances arises, has immediately notified the Purchaser in writing that it

	may claim such extension as caused by circumstances pursuant to above and upon request of the Purchaser, the Supplier/ IP shall substantiate that the delay is due the circumstances referred to by the Supplier/ IP. The Purchaser on receipt of such notice / appeal may agree to extend the Contract delivery date / completion period as may be reasonable and mutually agreed but without prejudice to other terms & conditions of the Contract. However, there would not be any revision in the Contract Price due to delay for reasons attributable to conditions mentioned above.
GCC 14.0	a) The Supplier/ IP will be liable to pay penalties/ liquidated damages in following, but not limited to, circumstances: The applicable rate for liquidated damages shall be 1% of the total price of licenses and implementation services as quoted by the supplier/ Implementation Partner in the price bid, for each week of delay until actual delivery or performance subject to a maximum deduction of 10% of the delayed goods/ services price. In such cases, Purchaser reserves right to terminate the Contract if amount of liquidated damages exceed this limit. The Purchaser will adjust such amount while making the payment to the Supplier/ IP. However, these liquidated damages will not be levied if the reason for delay is not attributable to the Supplier/ IP. b) Mis-declaration/ mis-representation of facts & figures (if detected at any point in time during bidding process or during currency of the Contract): The Purchaser shall recover from the Supplier/ IP, a sum equivalent to 10% (ten percent) of the total price for Licenses and Implementation Services for each of such cases. II. Failure to meet provisions of Service Level Agreement (SLA) as provided in Section 12 Clause 12.5 - Penalties in case of failure to meet Service Levels: 1. In case of problem categorized as "Severity 1": The Purchaser shall recover from the Supplier/ IP, a sum equivalent to 0.1% of the AMS price quoted for that year for every 30 minutes of delay over and above the given threshold limit for each of such incidents; 2. In case of problem categorized as "Severity 2": The Purchaser shall recover from the Supplier/ IP, a sum equivalent to 0.1% of the AMS price quoted for that year for every 60 minutes of delay over and above the given threshold limit for each of such incidents; and 3. In case of problem categorized as "Severity 3": The Purchaser shall recover from the Supplier/ IP, a sum equivalent to 0.1% of the AMS price quoted for that year for every 120 minutes of delay over and above the given threshold limit for each of such incidents. The decision of TSECL Steering Committee shall be final on levy/way-off of LD/ Penalty.
GCC 23.0	The successful bidder will be required to submit a Bank Guarantee (BG) equal to 3% of contract price from any Nationalized Bank / Scheduled Bank having a local branch office in **Agartala** as a guarantee of performance during the signing

	of agreement. The BG shall be in force for period of one month beyond the contract duration.
GCC 24.0	**The price adjustment shall be:** Prices shall not be subject to any upward revision on any account whatsoever throughout the period of contract. Provided that any revision in taxes, statutory levies, duties which is not occasioned due to any change in place, method and time of supply, or non-performance / non-fulfillment of any condition, or any exemption considered by the Bidder at the time of proposal, shall be considered for price adjustments.

6. Scope of Work

6.1. Overview

The Purchaser's objective is to engage or select CSP/MSP for providing Cloud Services for a period of 3.5 years for hosting the ERP system. The ERP system is covering the business functions which are indicated in subsequent paragraphs for process efficiency and better management. TSECL has successfully implemented the ERP solution covering its business functions which are indicated in subsequent paragraphs for process efficiency and better management. Bidders are required to critically review the purpose and requirements of hosting cloud servers and ensure inclusion of all essential goods & services (even if not mentioned specifically) for achieving the objective within the time frame for successful implementation.

Bidders should note that the specifications and functional requirements mentioned in the RFP are only minimum and indicative requirements within the broader functional areas. Bidder should supply, design and implement the solution appropriately keeping the business and statutory requirements of the Purchaser and functionalities available in the product.

Bidders should ensure that while designing and providing the complete solution to the Purchaser, instructions of Government of India, Government of Tripura or any other statutory authority applicable to Power Sector in India or the Purchaser such as norms, guidelines, standards etc., which are given time to time are complied with.

Bidders are also required to submit details and give confirmation on project delivery plan aspects like Architecture Diagram, Security Solutions, Storage sizing with input/output operations per second (IOPs), Project plan, Approach & Methodology for deployment on Cloud on Data Center & Disaster Recovery Site and Post Implementation support methodology for 3.5 years. Data Center Services are required for the environments namely Development (DEV), Quality (QA) and Production (PROD).

Further, the bidders need to implement and provide support of one standalone web-based application on Project Execution Management System (PEMS) as described in subsequent sections.

6.2. General Requirements

i. There should be sufficient headroom (at an overall level in the compute, network, and storage capacity offered) available for near real time provisioning (as per the SLA requirements of TSECL) during any unanticipated spikes in the user load.

ii. Ability to integrate fully with the Government of India approved Certificate Authorities to enable TSECL use the Digital Certificates / Digital Signatures.

iii. TSECL shall retain ownership of any user created/loaded data and applications hosted on CSP's/MSP's infrastructure and maintain the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

iv. TSECL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the TSECL's application. TSECL retains the right to request (or should be able to retrieve) full copies of these at any point of time.

v. TSECL retains ownership of its loaded software installed on virtual machines and any application or product that is deployed on the Cloud by TSECL.

vi. TSECL shall be provided access rights (including the underlying secure connection) to the user administration / portal of Cloud services to have visibility into the dashboard, SLAs, management reports, etc. provided by the Cloud Service Providers.

vii. CSP/MSP shall not provision any unmanaged VMs for the applications.

viii. CSPs/MSPs shall provide interoperability support with regards to available APIs, data portability etc. for TSECL to utilize in case of Change of Cloud Service Providers, migration back to in-house infrastructure, burst to a different Cloud Service Providers for a short duration or availing backup or DR services from a different service provider.

ix. CSPs/MSPs shall adhere to the ever-evolving guidelines as specified by CERT-In (http://www.certin. org.in/)

x. CSPs/MSPs shall also adhere to the relevant audit requirements as defined in the application document or any new requirement as published by Ministry of Electronics and Information Technology (MeitY) or Standardization testing and Quality Certification (STQC).

xi. CSPs/MSPs need to adhere to the guidelines and acts published by Government of India. No data should be shared to any third party without explicit approval by TSECL, unless legally required to do so by the courts of India. The CSP/MSP shall have to comply with the guidelines & standards as and when published by Govt. of India. CSP/MSP shall be responsible for all costs associated with implementing, assessing, documenting, and maintaining the empanelment, any guidelines published by MeitY shall be followed by the CSP. In case any misconduct is found, TSECL reserves the right to take appropriate legal course of action including blacklisting of the CSP/MSP

xii. CSP must have been Empaneled under the MEITY Cloud provider for minimum last 3 years; and must be empaneled for providing both GCC & VPC offering on cloud.

xiii. CSP must ensure individual VM level uptime SLA of 99.9%.

xiv. The DC & DR offered by the CSP must be on different seismic zone within India and must be min 500KM away from each other.

xv. TSECL retains ownership of the applications created for TSECL. TSECL retains the right to request (or should be able to retrieve) full copies of these at any point of time.

6.2.1. Statutory Compliance Scope

Any change or new requirement introduced in statutory compliance applicable to TSECL due to State or Central Government order during the tenure of the contract shall be considered as part of the scope of work.

6.3. Designing and Implementation

As part of designing & implementation methodology, bidder needs to submit the details of:

I. VM's sizing methodology needs to be confirmed by the bidder.

II. High Availability solution at different level from Network, Physical nodes, VM"s & Storage, having no single point of failure.

III. Proposed Solution should be compatible with IPv6 and High-level architectural diagram showing different layers of solution like Network, Security, Compute, Hardware, Storage & Backup layers.

IV. Proposed solution should have IP schema depicted at high level with netting to secure the applications directly getting exposed to Internet. Bidder should propose to deploy different applications and database in different VLANs with restricting users to directly access database layer and storage layer.
V. Backup solution with different features, like snapshots of VM‟s, online RDBMS backup (Standalone and Clustered), File system backups incremental and full back up of all data, restoration of data in test environment or as and when required.
VI. Compliance sheet for the features mentioned in the following section for Cloud specifications.
VII. DR solution and replication methodology
VIII. All product i.e. hardware and software should be deployed and used should be as per the Meity guidelines. TSECL reserve right to do the Physical audit of provided infrastructure and CSP is bound to disclose details of hardware and software.

6.4. Provisioning of Government Community Cloud (GCC)

Cloud Service Provider to setup complete environment to host ERP at DC (Production, Quality & Development) on – GCC Cloud & DR site. Bidder will be required to perform the following minimum technical tasks for the assigned areas:

i. Set-up Meity empaneled and STQC audit with VM‟s designated for individual ERP modules (DEV/TEST/PROD) with entire production environment in high availability mode.
ii. High Availability to be configured for Production environment by bidder including Guest VM OS cluster and integration of ERP Services in OS Cluster. Bidder to ensure High available nodes should not run on same physical host.
iii. Different VLAN's to be created to segregate front ending servers and database servers.
iv. Storage proposed for DC & DR should support IOPs as required.
v. All VMs offered should be Burstable VMs. VM's provisioned should have feature of auto-scalability of resources like vCPU& RAM without requiring any manual intervention or to reboot the VM, in case there is sudden traffic on the server or if the number of users increase then the VM should detect the incoming traffic and accordingly should scale the resources.
vi. The cloud service provider/Bidder should support TSECL & Idea Infinity in migrating the data from any offshore development center to Production environment in proposed Data Centre. Procedures and documentation to be developed for migration of applications, data & content. Hence, necessary connectivity needs to be provided by the bidder till the time of data migration.
vii. Bidders should propose & deploy firewall, load balancer, Antivirus, hardening operating system & Associated security solution to protect the VM's application, database from any type of external attacks like Virus attacks, DDOS attacks, hacking attempt, etc.
viii. The offered Network, security and associated components must be provided and should be available for future as a pick and choose option for TSECL in the published Marketplace of the Cloud service provider

Detailed Cloud Specifications and Features are given in further sections.

6.5. DR set-up with replication between DC & DR

Setting up of Disaster Recovery (DR) site after ERP is LIVE from primary Data Center (DC) Government Community Cloud solution. Bidder will be required to perform the following technical tasks for the assigned area:

i. The data-centers of Service provider should be separated in different geolocation in different seismic zone and not on same fault lines. The primary and DR site datacenters should be located in different state / UT with minimum 300KM Distance in between.
ii. Set-up Meity empaneled and STQC audit -Government Community Cloud to host ERP system at DR location.
iii. Proposed solution should support feature of resource scaling like vCPU, RAM within VM itself and creation of additional VMs depending on the kind of load coming on the application.
iv. The cloud platform should support scalability feature to handle load during normal & peak period. That is when users are accessing applications from DC, there will be no users accessing the applications from DR and so the only process on the servers at DR site would be of data replication, so the VM‟s to be proposed at DR site during normal scenario should be working at minimum resources say for e.g at 20% or 30% and should scale resources like vCPU & RAM when the load increases on VM‟s in DR site like during DR drills or when DR is LIVE. Once the DR drill is complete or primary DC is LIVE again, the VM itself should be able to scale down and continue to operate at minimum resources.
v. Setup replication between DC & DR
vi. Provide complete DR solution for production environment only, data replication plan and IT-Business Continuity Plan (IT-BCP) planning report along with ISO 22301 Certification
vii. Approach on how Bidder will meet the given Recovery Time Objective (RTO) & Recovery Point Objective (RPO).
viii. Propose replication monitoring tool to configure DR to be invoked with a single click.
ix. Generate reports to ensure RTO & RPO are met as per the set timelines
x. Bidder has to decide for DR Automation tool or Disaster Recovery management tool in order to match required RPO/RTO as per RFP.
xi. Proposed DR solution and Data replication methodology should be a proven solution for ERP applications.

6.5.1. DC-DR Failover & Restoration - Mock Drills / Actual Disaster

xii. The CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for complete switchover to DR.
xiii. The failover from primary DC to DR should be done through a proper DR announcement process which should be documented as part of BCP planning. In the event of a disaster, the system at proposed CSP's DR Data Center will be primary system.
xiv. The DR should be available (with its data) on-demand basis within the defined RTOs and RPOs, wherein 100% of the services of DC would run from DR site. All users of department will connect to CSP's system through Internet link.
xv. During the drill, the CSP shall demonstrate the fulfilment of SLAs at load of 100% users with 80% concurrency.
xvi. The use of Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance.
xvii. Application data and application states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. The installed application instance and the database shall be usable.
xviii. During the change from DC to DRC or vice-versa (regular planned changes), it should be as per the given RPO.CSP shall provide work flow based switchover/ failover facilities (during DC failure

& DR Drills). The switchback mechanism shall also be work flow based. The CSP shall also provide a tool/ mechanism for

xix. Department to trigger DR switchover, for example a "one-click DR". CSP shall provide support for the development and configuration of any additional scripts for

xx. successful working of DR.

xxi. The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data center. Users of application should be routed seamlessly from DC site to DR site.

xxii. Restoration provides an easy process for copying updated data from the DR server back to the DC server. Whenever main DC will be recovered and operational, the data from DR system to DC systems should be synchronized. Once this data is synchronized and verified, the switchover from DR system to DC system should be done. In that case all users will be accessing systems of main DC.

xxiii. CSP shall provide detailed DR activity plans which will contain steps/procedures to switch over services to DR site in the event of invocation of disaster at DC site.

xxiv. CSP shall also document steps for restoring services from DR site to DC site.

xxv. In case of failover to DR site (once disaster is declared) within the defined RTO, the SLA would not be applicable for RTO period only. Post the RTO period, SLA would start to apply and should be measured accordingly.

xxvi. The CSP shall conduct DR drill for FOUR days at the interval of not more than six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. The pre-requisite of DR drill should be carried out by CSP and department jointly. The exact process of the DR drill should be formulated in consultation with the department team in a way that all elements of the system are rigorously tested, while the risk of any failure during the drill is minimized. The process should be documented by the CSP as part of the disaster recovery plan. CSP shall plan the activities to be carried out during the mock drill and issue a notice to the department at least 15 working days before such drill.

xxvii. During the DR drill, the CSP need to arrange the full DR team with sufficient resources and expertise and complete the activity under the supervision of senior resource for co-ordination. The CSP shall develop appropriate policy, checklists in line with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate DR site.

Disaster Recovery			
Sr.No	Parameter	Target	Penalty
1.	RTO	2 hours	2% per additional hour of delay subject to a maximum delay of 4 hours beyond target.
2.	RPO	30 minutes	2% additional block of 15 minutes subject to a maximum delay of 60 minutes.
3.	Live Drill	• To be conducted every 6 months • Successful switch over and operation of application	Rs. 1000 for delay of each week, subject to a maximum of 5 weeks delay.

4	DR Live	• All operations to run LIVE from DR for atleast 15 Days every 6 months.	Rs. 10,00,000/- per day for not performing such Live operations from DR site. Running Live operations from DR site will be sole decision by the department and will inform Cloud service provider atleast 1 week before the Live date.

6.5.2. DR Managed Services

i. Provision for managed services for the entire DR facility will be required. CSP shall provide continuous maintenance activities to support the disaster recovery site. This includes (but not restricted to):
ii. CSP shall provide support for all server maintenance activities. This would include periodic health check, on-demand troubleshooting, repairs, part replacement etc. from certified vendors. ITIL processes named problem, change, incident & configuration will be followed by CSP at DR site.
iii. CSP should have proper escalation procedure and emergency response in case of failure/disaster at DC.
iv. CSP may partner with respective application / product support vendor to support DR in event of disaster or for performing periodic maintenance & upgrade activities
v. CSP shall perform RPO monitoring, reporting and event analytics and other activity associated with operations and management of DR plan and Implementation for the disaster recovery solutions.
vi. CSP shall provide a monitoring tool with dashboard showing RPO, RTO, changeover facility etc.
vii. The date, time, duration, and scope of each drill shall be decided mutually between department and the CSP. Extreme care must be taken while planning and executing DR drills to ensure that there is no avoidable service interruption, data loss, or system damage at DC.
viii. To demonstrate how the application fails over when the primary site goes down. The testing should include the:
ix. Uninterrupted replication to DR servers.
x. Lag in replication due to any unforeseen errors.
xi. Process of recovering from lags if any.
xii. Data integrity test of DR servers.
xiii. The CSP shall be responsible providing input for
xiv. Devising and documenting the DR policy discussed and approved by department.
xv. Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.
xvi. CSP shall support in bringing the machines to login level in case of disaster / DR drills. Provisioning, configuring, and managing FC-IP router for DC to DR replication in case the proposed solution requires FC-IP router.
xvii. The solution is envisaged for application level recovery scalable to site level recovery based on the impact of the disaster.
xviii. In case of reverse replication, since the DR site would be acting as main site, all the necessary support to run the environment has to be provided by the CSP.

xix. Reverse Replication is necessary and envisaged when the DR site is acting as the main site. The solution should ensure consistency of data in reverse replication till the operations are not being established at the Cloud site. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary Data Centre.

6.6. Implementation & Annual Maintenance Support of Project Execution Management System (PEMS):

Implementation & Annual Maintenance Support of Project Execution Management System (PEMS) as per workflow in Annexure "2" as a standalone web-based application without any integration / interface to existing ERP system operation in TSECL. Integration may be taken up on a later date which is beyond the purview of this NIT.

6.7. Reporting and Documentation

6.7.1. Reporting

i. Submit reports on a regular basis in a mutually decided format that is daily / Weekly and monthly uptime/downtime report. Softcopy of these reports shall be delivered automatically via email at specific frequency and to the pre-decided list of recipients.
ii. Submit information as part of periodic review as and when required by TSECL. Following is the indicative list of reports:
iii. Summary of component wise Data Centre uptime.
iv. Summary of changes in the Data Centre.
v. Log of preventive / scheduled maintenance undertaken.
vi. Configuration Management summary report.
vii. Change Management summary report.
viii. Service Level Management – priority/severity wise response and resolution.
ix. Service Failure Analysis, listing out escalations and downtime/outages, if any.
x. Incident Reporting
xi. Detection of security with the available solutions / workarounds for fixing.
xii. Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and the plan to fix the problems.
xiii. Standard Operating Procedure (SOP) for DC, System Documentation/ User manuals have to be prepared and maintained up to date with version control.
xiv. Provision to generate report in a mutually decided format for the proposed standalone web-based application.

6.7.2. Documentation

Preparation/ Updating of System Documentation of support requirements, upgrade, patching, cloning & migration in detail with version control. This will also include preparation of System document for complete infrastructure/facilities available in data center including Server, storage, network, network security configuration and deployments initially complete document and thereafter regular updating of the same with version controls. This documentation should be submitted as the project undergoes various stages of implementation. Indicative list of documents includes:

i. Detailed Project Plan

ii. Project Management Plan
iii. Details of complete solution deployed for TSECL in DC & DR sites including but not limited to all infrastructure deployed as part of Government Community Cloud, like IP schema, VM details, VLAN, storage LUN details, backup configuration and policies, network settings, firewall policies escalation matrix, BCP document, etc.

6.8. Help Desk Support

Bidder is required to create and maintain Help Desk / hotline that will resolve problems and answer queries related to any issues, problems, concerns occurring in Government Community Cloud including network connectivity, network security deployed in primary Data Center (DC) and disaster recovery (DR) site and its equipment supplied by the bidder & Support of Project Execution Management System (PEMS).
The help desk support to users shall be provided on 24*7*365 basis (Log issues via phone, ticket and online chat (24*7). The details regarding telephonic support will be carefully considered, as this will have effect on the support response to TSECL system end-users. The Bidders response and resolution time will be the basis for end- user support time in TSECL‟s service level agreements with the Bidder.

6.9. Post Implementation Support

Following maintenance support is required to be provided by the shortlisted bidder for a period of 3.5 years:

i. Complete monitoring and maintenance of DC & DR infrastructure, Cloud infrastructure, network, security, storage & backup, etc.
ii. Maintenance of Infrastructure Configuration Changes in the already implemented Modules.
iii. Provide 24x7, 365 days support for the entire solution including but not limited to proposed Cloud, storage, network, security and Backup solution proposed.
iv. Propose support and helpdesk system to allow TSECL users to call or log issues via phone, ticket and online chat (24x7).
v. Number of Phone calls, chats and tickets should be unlimited.
vi. Bidder to create and maintain all the necessary technical documentation, design documents, standard operating procedures, and configurations required to continued operations and maintenance of cloud services.
vii. Redundant Internet bandwidth along with security should be provided for smooth access of ERP applications with 99.5% uptime following Broad areas of services under this project.
viii. Support of Project Execution Management System (PEMS) for a period of 39 months post the implementation period of 3 months.

6.9.1. Server Administration & Maintenance

The bidder is expected to provide the Server Administration & Management services as follows:
i. Bidder shall provide the “Server Administration service" to keep servers stable, reliable and their operation efficient.

ii. Administrative support for user registration, User ID creation, maintaining user profiles, granting user access, authorization, user password support, and administrative support for print, file, and directory services.
iii. Setting up and configuring servers and applications as per configuration documents/ guidelines provided by TSECL.
iv. Installation/ re-installation of the server operating systems and operating system utilities.
v. OS Administration including troubleshooting, hardening, patch/ upgrades deployment, BIOS & firmware upgrade as and when required/ necessary for Windows, Linux or any other O.S proposed as part of this solution whether mentioned in the RFP or any new deployment in future.
vi. Ensure proper configuration of server parameters, operating systems administration, hardening and tuning.
vii. Regular backup of servers as per the backup & restoration policies stated by TSECL from time to time.
viii. Regularly monitor and maintain a log of the status of critical services, performance of servers including but not limited to monitoring of CPU, disk space, memory utilization, I/O utilization, etc.
ix. Regular analysis of events and logs and maintain the reports for future audit purposes.
x. Managing uptime of servers as per SLAs.
xi. Take appropriate steps to comply with the audit observations made by various internal/ external auditors.
xii. Depending on the nature of applications deployed, Bidder shall suggest/ implement appropriate security measures on various servers, especially the Web, Application and Database servers.
xiii. Co-ordinate with SSL Certificate vendor for issuing and deployment of SSL certificates.
xiv. Preparation/ updating of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening.

6.9.2. Storage Administration & Management

i. Installation and configuration of the storage disk to VMs at Data Centre and DR Site.
ii. Management and monitoring of storage environment to maintain performance at desired optimum levels.
iii. Preparation of Standard Operating Procedure (SOP) document for the Storage and SAN Administration
iv. Configuration and provisioning of storage whenever a new application is hosted in the Data Centre and at DR Site. This shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc.
v. Bidder shall provide L1, L2, L3 & subject matter expert level of support for any issues related to proposed storage infrastructure to TSECL at primary Data Centre and DR site. Bidder will coordinate with TSECL and ERP implementation vendor to resolve any storage / IOPS performance related issues as per SLA.
vi. Compliance to IT Security policies of TSECL/ Statutory bodies.
vii. Adherence and maintenance of the user access controls as advised by TSECL.

6.9.3. Network and Security management Service

i. Cloud Service Provider will have to provide complete managed services for all networking components proposed as part of the solution like, vSwitches, routers, vFirewall, load balancers and links.
ii. Configure, manage & modify configuration of the network devices / vFirewall etc. policies as and when required.
iii. All the security devices are virtual and should be dedicated to TSECL.

6.9.3.1. Internet and Web Security Administration

i. Coordination with ISPs for installation / configuration of links
ii. Monitoring of Internet links and co-ordination with ISPs for restoration of failed link(s).
iii. Monitoring bandwidth utilization.
iv. Carrying out configuration changes on router as per the TSECL requirements.
v. To ensure working of all the TSECL's URLs and Internet applications from outside TSECL's Intranet.
vi. Backup /restoration/synchronization of configuration files of devices.
vii. Maintaining static NAT table of ISPs.
viii. Installation/configuration/management/up gradation of the devices / appliances.
ix. Public IP management and DNS management
x. DNS redirection during DR Drill

6.9.3.2. Antivirus Management

AV Management service includes virus detection, eradication, and synchronization across devices and support for required security classifications. The scope of services is applicable to all the nodes, all current and future versions of the Anti-virus S/W:

i. Support for virus control and loading of antivirus patches/ signatures as and when available.
ii. Installation/ up gradation/ support of Antivirus software clients.
iii. Ensure all the servers updated with the latest virus definition.
iv. Problem analysis and its resolution related to Antivirus software.
v. Periodic review and reporting of logs and corrective action.
vi. Diagnose and rectify any virus/worm problems, which can be fixed by the anti-virus tool.
vii. Provide feedback to TSECL on any new viruses detected or possible virus attack and take up promptly with Support vendor for getting the appropriate patch and carry out the timely maintenance.
viii. Guide/suggest TSECL on the effectiveness of anti-virus management and alternate remedial action, if any.

6.9.4. Backup/Restore management for Servers, Database, Applications etc.

i. To perform backup and restore management in coordination with TSECL's policy & procedures for backup and restore, including performance of daily, weekly, monthly, quarterly and annual backup functions (full volume and incremental) for data and software maintained on the servers and storage systems using Enterprise Backup Solution.
ii. Backup and restoration of Operating System, application, databases and file system etc. in accordance with defined process / procedure / policy.
iii. Define backup architecture and mechanism (SAN/LAN/Object Storage) to meet TSECL's requirement

iv. Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
v. Ensuring prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.
vi. Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
vii. Media management including, but not limited to, tagging, cross-referencing, storing (both on-site and off-site), logging, testing, and vaulting in fireproof cabinets.
viii. Installation, re-installation, upgrade and patch deployment of the Operating System in the event of hardware/ Software failure, OS issues, release of new version or patches by the OEM etc.
ix. Generating and sharing backup reports periodically.
x. Coordinating to retrieve off-site media in the event of any disaster recovery.
xi. The CSP would be the owner of Backup media and TSECL will not provide any media for Backup.
xii. Periodic Restoration Testing of the Backup.
xiii. Maintenance log of backup/ restoration.
xiv. Update/ Maintain Standard Operating Procedure (SOP) documents.

6.9.5. Testing Planning

Once Government Community Cloud is deployed, data is exported/imported in DR servers, the testing of application at DR site becomes very important. Therefore, the bidder has to perform following testing:

6.9.5.1. Infrastructure Testing

The bidder should perform various testing on Infrastructure provided at DR site. This should include following thing:

- Disk IO testing.
- Network throughput testing
- CPU and RAM benchmarking testing
- Read/Write latency testing.
- Dry Run of DR drill

This should also include the following but not limited to:
Inclusion of "Backup/Restore, Virtualization, Cloud provisioning, Replication and Reverse Replication etc.

6.9.5.2. Functional Testing

Once the data is replicated to DR site and application started functioning, the functional testing of Application will be done by TSECL Team along with Application vendors. The bidder requires to provide support and co-ordination in this case. TSECL and application vendors may perform following testing.

- Software Module testing as per functional requirement.
- User authentications testing.
- Users add/delete, reports generations
- Heavy application transactions on DR servers.
- Backup exports
- Backup restoration and so on.

6.9.5.3. Data Integrity Testing

Data Integrity will be very important and crucial factor in overall process. Data integrity testing will be performed by TSECL IT staff and application vendors which would include:

i. Amount of data verification at both ends
ii. Table size and records testing.
iii. User's status at both ends.
iv. Invoices/transactions verification at both ends.
v. Data in log files.

6.9.5.4. Service Maintenance

The bidder requires to maintain the infrastructure at DR site as per the scope mentioned in scope of work in section 7. Reporting for DR site should be as per the section 7.6

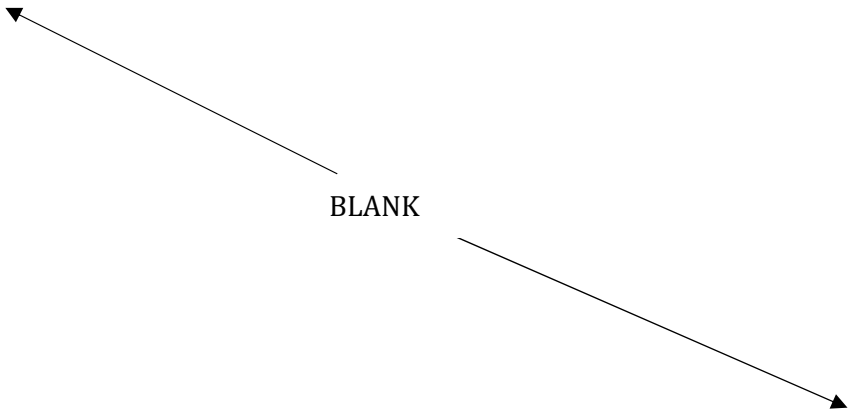
i. Monitoring of Replication status.
ii. Lag in replication due to any unforeseen errors.
iii. Network monitoring
iv. Security monitoring and analysis
v. Reporting if any issue is arising in replication.
vi. Daily backup at DR end

6.9.6. Failover

In the event of disaster, the ERP system at Proposed Bidder's DR site will become primary system. All users of TSECL will connect to Bidder's DR site through Internet/MPLS/P2P link. Since the ERP systems has been asked on cloud infrastructure, all systems should be auto scalable. Whenever load of users will grow, the ERP systems should scale resources automatically in terms of RAM and CPU and once the DC is LIVE then reverse replication should be configured and DNS records to be changed and Operations should be transferred to Primary Site (DC), post this the resource utilization like vCPU& RAM should be back to minimum requirement. The failover from Main DC to DR should be done through a proper DR announcement and informing all stakeholders. DR portal should have self-service ability to kick off various tasks including failover and failback.

6.9.7. Restoration

Restoration provides an easy process for copying updated data from the DR server back to the DC server. Whenever main DC will be recovered and operational, the data from DR system to DC systems should be synchronized. Once this data is synchronized and verified, the switchover from DR system to DC system should be done. In that case all users will be accessing ERP systems of main DC



7. Evaluation Details

7.1. Guidelines to Bidders

i. Financial requirement/ certification of only the bidder will be considered and financials of parent company / holding company etc. will not be considered. Consolidated financial statements of the bidders will also not be considered.
ii. Bidder should be Authorized representative/ Service Provider of respective Cloud Services.
iii. If any project / contract involves multiple subsidiaries, it will be treated as only one credential / experience.
iv. All credentials of Bidder as Lead Bidder/Prime Bidder will only be considered
v. Cut-off date for calculating number of years shall be the date of bid submission
vi. The Purchaser will have the right to independently contact and verify the accuracy of credentials with Bidder's end-client. Bidder will have to provide necessary details as per the requirement of the Purchaser.
vii. All Documents related to bidder's experience should be in English language. If not, document in original language along with its English translation (certified by bidder's Company secretary) should be submitted.

7.2. Pre-Qualification Requirements

7.2.1. For CSP

S.No.	Criteria	Documentary proof to be submitted
1	Cloud Service Provider (CSP) should be a company registered under Indian Companies Act 1956.	Certificate of incorporation along with PAN
2	A CSP should have minimum average annual turnover of at least 150 Crore each in last three audited financial years (FY 2019-2020, 2020-2021 & 2021-2022).	Certificate from Company Secretary / Auditor / CA
3	The Cloud Service Provider should be empanelled with Ministry of Electronics and Information Technology (MeitY), Govt. Of India for providing DC / DR services, website (http://meity.gov.in/content/gicloud-meghraj) for Cloud Service providers (CSPs) a. The CSP should be MeitY empanelled for last 3 years minimum) and must have 3 Meity empanelled DCs in India (as on bid submission date). b. The proposed Data Centres should be within India.	Empanelment letter from MeitY AND Valid copies of proof attested by authorized Bid signatory

	c. The proposed Data Centres should be successfully STQC audited. d. The proposed Data Centre should have option of Government Community Cloud (GCC) for a period of minimum 3 years.	
4	CSP should have executed at least 5 projects of DC/DR with Cloud deployment (ERP Software/Govt Application Hosting/ SAP Application / SAP HANA / S4H Hana Application, Microsoft Dynamics ERP) with cumulative order value of minimum INR 5 Cr. Out of these 3 projects, minimum 2 should be from any State / Central Government Entity (PSU / Power Utilities) within last 5 years.	Purchase order / LOI (any MSP)- Customer names and contact for Ref Check if the CSP does not have direct order from customer and PO is picked by MSPs
5	The CSP must not be banned or debarred or blacklisted by any State Govt. / Central Govt. / Central or State Govt. Undertakings / Utilities / Private Organizations etc. as on bid submission date.	Declaration/Undertaking in this regard by the authorized signatory of the Bidder needs to be submitted
6	The CSP must not have been declared insolvent/ bankrupt or should not have filed for insolvency/ bankruptcy or in the process of being declared bankrupt before any designated authority	A Self Declaration/Undertaking regarding Bidder company not being bankrupt shall be submitted.
7	The CSP/MSP must have strength of at least 100 IT Professionals (data centre/networking/system administration/ cloud services professional's/cloud security experts) on their payroll as on date of submission of this bid. At least 10 of these professionals must have experience (of minimum 5 years) in deployment and Management of cloud solution/ DR Management / virtual server administration/system administration, Virtualization, security, database etc.)	Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the bid as per the requirement.
8	The Offered DC & DR should be in Different State/UT of India with min distance of 300KM. The CSP must be ISO 22301 Compliant for Business Continuity aspect.	ISO Certificate and Declaration
9	The CSP should possess all the below certifications which are valid as on bid submission date: - ISO 27001:2013 certification	Copies of valid certificates as on bid submission date

	- ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology - ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds - ISO 20000-1:2011 certification for Service Management System - PCI DSS -compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud - SOC 1, 2, 3 for Security - Conform to at least Tier III standard, certified under TIA 942 or Uptime Institute certifications by a 3rd party	
10	The CSP should provide all variants of cloud service – Infrastructure as a Service (IaaS), --Platform as a Service (PaaS) --Software as a Service (SaaS) -- GCC (Government Community Cloud)	Self Certificate with Public Link/Documentation

7.2.2. For MSP

S.No.	Criteria	Documentary proof to be submitted
1	MSP should be a company registered under Indian Companies Act 1956.	Certificate of incorporation along with PAN
2	MSP must have average annual revenue of INR 150 Crores or more for each of the last Three financial years (FY 2019-2020, 2020-2021 & 2021-2022).	Certificate from Company Secretary / Auditor / CA
3	The MSP must be the lead bidder for this tender. The MSP should have executed at least 3 Cloud based infrastructure and application Managed Services. One of these projects must be for Government / PSU utilities in India.	Purchase order / LOI and Performance certificate/mail from the client. In cases where Purchase order/ LOI/ Performance certificate/mail is not available bidder needs to

		provide self-certificate signed by bid authorized signatory on bidders letter head.
4	The MSP must not be banned or debarred or blacklisted by any State Govt. / Central Govt. / Central or State Govt. Undertakings / Utilities / Private Organizations etc. as on bid submission date.	Declaration/Undertaking in this regard by the authorized signatory of the Bidder needs to be submitted
5	The MSP must not have been declared insolvent/ bankrupt or should not have filed for insolvency/ bankruptcy or in the process of being declared bankrupt before any designated authority	A Self Declaration/Undertaking regarding Bidder company not being bankrupt shall be submitted by the authorized signatory
6	Confirmation from CSP about agreeing to work together and associate for this RFP/opportunity	The bidder must enclose a declaration from CSP that the MSP will comply to work together and should submit an authorization certificate from the original CSP that the MSP is ready to associate with them for this opportunity
7	Undertaking of no Conflict of Interest (The bidder shall submit a self-declaration/undertaking that it has no potential conflicts of interest of interest that exist, arise or may arise (either for bidder or its team) in the course of performing the service. The bidder shall strictly avoid conflict of interest with other assignments)	A Self-Declaration / Undertaking by the authorized signatory of the Bidder needs to be submitted
8	The MSP should have CMMI level 3 including ISO 9001:2003, ISO 27000, ISO 20001, ISO 14000 certified.	Copy of relevant certificates to be enclosed.

Note: In case of global credentials, the supporting documents should be provided in English language.

7.3. Technical Qualification Criteria

The technical Bids along with all the supporting documents shall be submitted in separate folder. Department will review the technical bids of the CSP to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at department's discretion. The CSP's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and technical evaluation framework. Each Technical Bid will be assigned a technical score out of a maximum of 100 marks. Only the bidders who get an aggregate technical score of 70% or more will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid and Bidder.

#	Compliance	Marks	Documents Required
MSP/CSP Turnover	The average turnover in Indian Rupees for last THREE (3) FY 2019-2020, 2020-2021 & 2021-2022 audited financial Year should be minimum 500 Crores from Indian IT Business in cloud. (Excluding hardware trading).	50 Crores – 5 Marks 51 - 100 Crores – 7 Marks Above 100 Crores – 10 Marks	MSP can provide Published Audited Annual reports for FY 2019-2020, 2020-2021 & 2021-2022.
MSP/CSP Certifications	CSP should be certified with following certificates (valid copy to be provided) 1. PCI DSS 2. ISO 27001 3. ISO 20000-1 4. ISO 22301 5. ISO 27017 6. ISO 27018 7 TIA Tier III 8. SOC 3 9. TIA 942 10. ISO 9000:2015	<=5 Certification: 5 Marks, > 5 Certification, 5 marks for each additional certificate, Maximum 15 Marks. (E.g.: CSP 1: 3 Certificate- 0 Marks, CSP 2: 7 certificate- 4 Marks, CSP 3: 10 certificate- 10 Marks)	Copy of certification
TRS & FRS	The requirement for Technical and Functional requirement compliance matrix under section named "Technical and Functional Compliances" provided along with this tender. Bidder is expected to indicate compliance in "1" for Yes and "0" for No against all the requirements. Scoring for this format will be done based	96% - 100%: 15 marks 90%-95%: 10 marks 80% - 89%: 7 marks < 80%: 5 marks	Filled up technical compliance sheet

	on compliance by bidder for each point vis-à-vis total number of points.		
O&M	MSP should have technical staff with following skill sets (System (Windows, Linux)/Network/ Database/ Security Administrators, Middleware / Application technical support experts, etc.)	<100: 0 Marks 101-200: 5 Marks 201 - 300: 7 Marks More than 300: 10 Marks	Statement by bidder on bidder's letter head signed by authorized bid signatory.
MSP/CSP Experience	The Bidder have successfully completed / Currently hosting application and infrastructure managed services on cloud for any Govt. organization/ PSU in India in last seven financial years with a minimum order value of 5 Crores.	=2: 5 Marks >2 to <= 3 projects: 10 Marks >4 projects: 20 Marks	Performance Certificate / mail from the client. In cases Performance certificate / mail is not available bidder needs to provide self-certificate signed by bid authorized signatory on bidders letter head.
Office	MSP having office in North East with Manpower. Documentary evidence for the same to be provided.	10 Marks	Rent agreement copy along with declaration on letter head.
ERP	MSP/CSP having experience in hosting ERP in North East of min value 5cr in last 3yrs	10 Marks	PO copy or LOI of customer.
Capability	Technical Presentation and Quality of Proposal (Points for presentation are mentioned below). Presentation should be strictly made on the given points.	10 Marks	
Total Marks		100	

The bidder should cover following points in Technical Presentation (Should not be more than 10 slides):

- Proposed Cloud Architecture.
- Business Continuity Plan.
- Proposed Security Architecture.
- Major risks for the project & Mitigation plan for each of these risks.
- Migration Strategy

8. Evaluation Process

Evaluation shall be done based on the information provided in the technical proposal (& subsequent clarification, if any) and Clarifications / Answers given by the bidders to department during the Presentation and Site visit.

The evaluation will be done based on QCBS (Quality cum Cost Based Selection) and on the parameters given below:

Bidders those have secured the minimum 70% in the Technical Evaluation i.e. section 1 & 2 individually will be advised of the location, date, and time set for opening of commercial proposal. Adequate notice will be given to allow interested bidders or their representatives to attend the opening of the commercial proposals.

Technical evaluation will be done based on the below calculations.

Formula;

$$\frac{\text{Combined marks of the respective vendor}}{\text{Total Technical Marks (100 Marks)}} \times 100$$

Technical Score Marks x Technical W'tage i.e. 70

$$\text{CSP 1} = \frac{\text{80 Marks}}{\text{100 (Out of)}} \times 100 = 80.00 \qquad 80.00 \times 0.7 = 56.00$$

Bidder	Combined Marks (A)	Out of (B)	Tech Marks (TM)= A/B*100	Tech. W'tage TW = 0.7	Tech. Marks TMW = TM x TW
CSP 1	80	100	80.00	0.7	56.00
CSP 2	85	100	85.00	0.7	59.50
CSP 3	78	100	78.00	0.7	54.60

8.1. Commercial Evaluation Criteria

Commercial evaluation will be done based on the below calculations.

The evaluation process shall consider the "Total Contract Value" Vendor proposing lowest TMO shall be given a commercial score of 30. Commercial score for other vendors will be calculated as under:

For example, if we have CSP 1, 2 and 3 quoting rates as given below:

#	Item	CSP 1	CSP 2	CSP 3
P1	Cloud infrastructure DC & DR Site (Compute, Storage, Software's, Tools Networking and security)	3,00,00,000	4,00,00,000	3,00,00,000
P2	Managed Services – OS, DB, Backup, Network, Security, Mock Drill, Replication & Monitoring	3,00,00,000	2,00,00,000	3,00,00,000
P3	Optional component in the rate card	2,00,00,000	1,00,00,000	3,00,00,000
Total Project Value for the 3.5 Yrs. Without Taxes		8,00,00,000	7,00,00,000	9,00,00,000

The overall commercial score will be determined on basis of formula given below, following which the bidder with the highest score will be awarded the contract.

- Formula:

$$\frac{\text{Lowest Total Contract Value}}{\text{Price quoted by CSP2}} \times 100$$

Commercial Marks (CM) x Commercial W'tage i.e. 0.3

$$\text{CSP 1} = \frac{7,00,000}{8,00,000} \times 100 = 87.50 \qquad 87.5 \times 0.3 = 26.25$$

Bidder	Total Contract Value in Rs. (A)	Lowest Contract Value (B)	Commercial Marks (CM)= B/A*100	Commercial W'tage CW = 0.3	Commercial Marks CMW = CM x CW
CSP 1	8,00,000	7,00,00	87.50	0.3	26.25
CSP 2	7,00,000	7,00,00	100.00	0.3	30.00
CSP 3	9,00,000	7,00,00	77.78	0.3	23.33

8.2. Final evaluation

Technical and Commercial score will be added to arrive at Total Score out of hundred. The proposal securing the highest combined score will be ranked as H1, Second highest as H2 and Third Highest as H3.

Example:

As per the above example, three proposals with combined Technical and Financial evaluations score would be ranked as under:

Final evaluation based on technical score and financial score is as follows:

CSP	Tech. Marks TMW (0.7)	Commercial Marks CMW (0.3)	Total TMW + CMW	Highest Scope
1	56.00	26.25	82.25	H2
2	59.50	30.00	89.50	H1
3	54.60	23.33	77.93	H3

***Based on the above matrix the contract will be awarded to CSP 2, as CSP 2 has the highest score (H1) of 88.83 marks.

8.3. Technical Specifications

8.3.1. CSP Technical and Functional Compliances (TRS & FRS)

Bidder must fill up the following compliance table for cloud and website/portal requirements. Compliance against these heads would imply compliance against all parameters / activities mentioned under respective heads below. These requirements are mandatory and in case of non-compliance, the Bidder may not be qualified for commercial evaluation at the discretion of TSECL.

Bidder must fill up the following compliance table for cloud and website/portal requirements. Compliance against these heads would imply compliance against all parameters / activities mentioned under respective heads below. These requirements are mandatory and in case of non-compliance, the Bidder may not be qualified for commercial evaluation at the discretion of TSECL.

Sr.	Section	Description	Compliance (Yes / No)
1	13.1	Cloud Portal Capabilities	
2	13.2	General Cloud Requirements	
3	13.3	Disaster Recovery Management	
4	13.4	Cloud Service Provisioning Requirements	
5	13.5	Data Management	
6	13.6	Operational Management	
7	13.7	Cloud Network Requirements	
8	13.8	Cloud Data Centre Specifications	
9	13.9	Cloud Compatibility Requirement	
10	13.10	Cloud Security Requirements	
11	13.11	Virtual Machine Specifications	
12	13.12	Cloud Resource and Network Monitoring	
13	13.13	Application Performance Monitoring	
14	13.14	Web Application Firewall as Service	
15	13.15	Malware monitoring services, Application Audit, External Vulnerabilities	
16	13.16	Managed Services	
17	13.17	Database services	
18	13.18	Helpdesk Support from Cloud Service Provider	
19	13.19	SIEM Service	

1.1 Cloud Portal Capabilities: -

Sr.	Cloud Capabilities	Compliance(Y/N)	Remarks
1	In order to increase the service availability, the cloud service provider must offer multidimensional auto-scaling of cloud services where resource like RAM and CPU will scale vertically as well systems should scale horizontally		
2	Cloud service should enable to provision cloud resources through self service provisioning interface.		
3	Cloud System should enable to provision cloud resources from application programming interface (API)		
4	Cloud System should be accessible via secure method using SSL certificate.		
5	Should be able to create, delete, shutdown, reboot virtual machines from Cloud portal.		
6	Should be able to size virtual machine and select require operating system when provisioning any virtual machines		
7	Should be able to predict billing of resources before provisioning any cloud resources if integrated with billing system.		
8	Should be able to set threshold of cloud resources of all types of scalability.		
9	Should be able to provision any kind of resources either static or elastic resources.		
10	The cloud virtual machine created by portal should be have at-least two virtual NIC cards. One NIC card should be used for internet traffic while other should be used for internal service traffic.		
11	The Cloud System shall be capable of allowing applications to self-service compute, network and storage infrastructures automatically based on workload demand.		
12	Should ensure that the virtual machine format is compatible with other cloud systems.		
13	Cloud System should give provision to import cloud VM template from other cloud systems.		
14	Cloud System should support provisioning from self-Cloud Orchestration System to add more storage as and when require by VM.		
15	Cloud System should give provision to attached new block disk to any cloud VM from self-service portal.		
16	The cloud virtual machines should be scalable in terms of RAM and CPU automatically without reboot.		
17	Cloud System must support multi-tenancy for management perspective. Different department or group company should be able to access allocated resources only.		
18	The Solution should provide a simple to use intuitive web end experience for Cloud Administrator and User Departments.		
19	The Solution should provide Unified Infrastructure management with complete inventory management of virtual machines & physical resources.		
20	The Solution should provide comprehensive service catalog with capabilities for service design and lifecycle management, a web-based self-service portal for users to order and manage services.		

Sr.	Cloud Capabilities	Compliance(Y/N)	Remarks
21	Cloud System should have provision to ensure that cloud virtual machine is into separate network tenant and virtual LAN.		
22	Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM		
23	Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM.		
24	Cloud System must ensure the ability to map private IP address of cloud VM to public IP address as require from portal of Cloud Orchestration System.		
25	Should support use of appropriate load balancers for network request distribution across multiple cloud VMs.		
26	Cloud Orchestration System should provide network information of cloud virtual resources.		
27	Cloud Orchestration System should have built-in user-level controls and administrator logs for transparency and audit control		
28	Cloud System should support policy based provisioning of virtual machines. Based on granted permission, users should be able to perform the operations. For example if any users doesn't have permission to delete VM, he should not be able to do it.		
29	Cloud System should support quota based system. Users should not be able to provision resources beyond allocated quota.		
30	The Admin should be able to define Access Control to Permit or Deny operation per Group or per User.		
31	Should have provision to define Workflow to Escalate Permission to Group Admins or System Admins.		
32	The Solution should allow for implementing workflows for provisioning, deployment, Decommissioning all virtual and physical assets in the cloud datacenter.		
33	User Management: The solution shall provide comprehensive user management		
34	Functions including tenant-specific user grouping and admin/user rights within the scope of a tenant. The tenant-admin user is considered distinct from the overall cloud solution administrator. The tenant-admin shall be able to manage own profile, tenant preferences, as well as users within the tenant/group scope. Individual users shall be able to manage their own profile and individual preferences. The solution administrator shall have the rights to all User Management functions.		
35	Cloud System should provide facility to make template from virtual machines.		
36	Cloud System should give provision to make clone of cloud virtual machine from Cloud Orchestration System.		
37	Cloud System should have provision to live migration of virtual machine to another physical servers in case of any failure.		
38	Cloud System cloud shall continuously monitor utilization across Virtual Machines and shall intelligently allocate available resources among the Virtual Machines.		

Sr.	Cloud Capabilities	Compliance(Y/N)	Remarks
39	The Cloud System solution shall be able to dynamically allocate and balance computing capacity across collections of hardware resources of one physical box aggregated into one unified resource pool.		
40	The Cloud System cloud solution should support detecting, in real time, resource requirements of a system in virtual environment and automatic scaling of resource parameters like RAM and CPU to compensate resource requirement in a system.		
41	The solution shall provide near zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.		
42	Cloud System should give provision to monitor the network traffic of cloud virtual machine.		
43	Cloud System should offer provision to analyze of amount of data transferred of each cloud virtual machine.		
44	Cloud System must offer provision to monitor uptime of each cloud virtual machine.		
45	Cloud System must make provision of resource utilization graph i.e. RAM of each cloud virtual machine. There should be provision to set alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.		
46	Cloud System must make provision of resource utilization i.e. CPU graphs of each cloud virtual machine.		
47	Cloud System must make provision of resource utilization graph i.e. disk of each cloud virtual machine. There should be graphs of each disk partition and emails should be sent if any threshold of disk partition utilization is reached.		
48	Cloud System must give provision to monitor the load of Linux/Windows servers and set threshold for alerts.		
49	Cloud System must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.		
50	Cloud System must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity		
51	Should be able to create virtual instances of required configuration without limiting to any standard templates		

1.2 General Cloud Requirement: -

Sr.	Description	Compliance Y/N	Remarks
1	TSECL intends to avail a managed Meity Government Community cloud for hosting “the Portal” at the Bidder’s Data-Center.		
2	The data-center shall be at least a Uptime/TIA 942 certified Tier III data-center providing 99.9% services availability SLAs		
3	The data-center shall be well equipped with physical, logical, network and infrastructure security solutions, access protection systems including physical access control, and shall maintain the logs of the access.		

Sr.	Description	Compliance Y/N	Remarks
4	The data-center shall be well equipped with intrusion detection & protection systems, firewalls, system management solutions & tools, back-up & restore solutions, monitoring tools, network load balancer for applicable servers and network layer security to isolate the TSECL Web, App and DB environment		
5	The data-center shall have ability to scale up or down the servers/compute resources on-demand/ as desired without significant down time.		
6	The compute infrastructure shall include the physical / virtual machines, operating systems, application servers, database server, anti-virus solutions and system management & back-up agents.		
7	The IT infrastructure should be hosted on Government Community Cloud. The cloud should have following capabilities:		
8	All the virtual machines should be auto scalable in terms of RAM and CPU.		
9	The cloud platform should be enough intelligent to predict incoming load and assign resources to virtual machines dynamically without rebooting system.		
10	Cloud platform should always allocate minimum 50% buffer resources against running load to handle sudden spikes.		
11	The cloud platform should provide high availability across virtual machines so that even if any host goes down, all guest virtual machines should be migrated to another host automatically.		
12	Cloud platform should support horizontal load balancing along with vertical. Load balancer should be used to load balance traffic. Load balancer should be able to trigger new virtual machines to handle additional load. If load goes down, newly triggered virtual machines should be recycled.		
13	Cloud provider should give TSECL a dashboard of all virtual machines to monitor allocated and used resources by the portal application.		
14	Cloud dashboard should allow to generate reports for trend analysis of system usage.		
15	TSECL team should be able to get the console access of any virtual machines if require.		
16	There should be provision to generate historical reports of resources utilization.		
17	There should be admin panel to create, delete, start, stop, and copy virtual machines.		
18	There must be provision to create golden image of virtual machine so that it can be used to make more machines of same configuration.		
19	There should be provision to take snapshots of machines so that working images of testing/quality machines can be taken.		
20	Security Advisor- The CSP should have an in-built mechanism of notifying the security threats to the end user by continuously monitor the security of machines, networks, and Azure services using hundreds of built-in security assessments or create customize policy. Use actionable security recommendations to remediate issues before they can be exploited.		

1.3 Disaster Recovery Management: -

Sr.	Description	Compliance Y/N	Remark
1	Service Provider would be responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center and meet the RPO and RTO requirements.		
2	RPO should be less than or equal to 30 minutes and RTO shall be less than or equal to 2 hours		
3	However, during the change from Primary DC to DR or vice-versa (regular planned changes), there should not be any data loss.		
4	There shall be asynchronous replication of data between Primary DC and DR and the CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.		
5	During normal operations, the Primary Data Center will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site.		
6	In the event of a site failover or switchover, DR site will take over the active role, and all requests should be routed through DR site. The pre-requisite to route request to DR should be articulated properly and shared by service provider.		
7	Whenever there is failover from primary DC to secondary (DR), compute environment for the application at DR site shall be equivalent to DC including all the security features and components of DC, without the failover components.		
8	The installed application instance and the database shall be usable and the same SLAs as DC shall be provided.		
9	The bandwidth at the DR shall be scaled up to the level of Data center when DR is activated.		
10	The service provider shall conduct live DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DR or vice-versa (regular planned changes), there should not be any data loss. The pre-requisite of DR drill should be carried out by service provider and TSECL jointly. Certificate for DR drill should be submitted to TSECL for compliance.		
11	The service provider shall clearly define the procedure for announcing DR based on the proposed DR solution. The service provider shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The service provider shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Bank at least two weeks before such drill.		

Sr.	Description	Compliance Y/N	Remark
12	The disaster recovery plan needs to be provided by the service provider which needs to be updated half-yearly.		
13	The service provider should offer dashboard to monitor RPO and RTO.		
14	Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.		

1.4 Cloud Service Provisioning Requirements: -

Sr.	Description	Compliance Y/N	Remark
1	The Service provider should offer cloud service provisioning portal for in order to provision cloud services either via portal, mobile app or automated using API.		
2	Cloud service provider should enable to provision / change cloud resources through self service provisioning portal.		
3	Service provider should enable to provision / change cloud resources from application programming interface (API).		
4	The user admin portal should be accessible via secure method using SSL certificate.		
5	Should be able to take snapshot of virtual machines from provisioning portal.		
6	Should be able to size virtual machine and select require operating system when provisioning any virtual machines.		
7	Should be able to predict his billing of resources before provisioning any cloud resources.		
8	TSECL should be able to set threshold of cloud resources of all types of scalabilities.		
9	Should be able to provision all additional storages required for cloud services.		
10	Should be able to provision any kind of resources either static or elastic resources.		
11	Should get list of all cloud resources from provisioning portal.		
12	Should be able to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load.		

1.5 Data Management: -

Sr.	Description	Compliance Y/N	Remark
1	Service provider should always ensure that data is destroyed whenever any cloud virtual machine is recycled or deleted. The data destruction policy of service provider should be shared with TSECL before.		
2	Service provider should clearly define policies to handle data in transit and at rest.		

3	Service provider should not delete any data at the end of contract period without consent from TSECL.		
4	In case of scalability like horizontal scalability, the service provider should ensure that additional generated data is modify/deleted with proper consent from TSECL.		
5	Service provider should ensure secure data transfer between PDC and DR site.		
6	Service provider shall put in place a system to prevent data leakage protection and prevention.		

1.6 Operational Management: -

Sr.	Description	Compliance Y/N	Remarks
1	Service provider should upgrade its hardware time to time to recent configuration to delivery expected performance for TSECL.		
2	Investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools.		
3	Service provider should manage their cloud infrastructure as per standard ITIL framework in order to deliver appropriate services to TSECL.		
4	Service provider should deliver cloud having method and system for real time detection of resource requirement and automatic adjustments.		

1.7 Cloud Network Requirements: -

Sr.	Description	Compliance Y/N	Remarks
1	Service provider must ensure that cloud virtual machine of TSECL is into separate network tenant and virtual LAN.		
2	Service provider must ensure that cloud virtual machines are having private IP network assigned to cloud VM.		
3	Service provider must ensure that all the cloud VMs are in same network segment (VLAN) even if they are spread across multi datacenters of Service provider.		
4	Service provider should ensure that cloud VMs are having Internet and Service Network (internal) vNIC cards.		
5	Service provider should ensure that Internet vNIC card is having minimum 1/10 Gbps network connectivity and service vNIC card is on minimum 10 Gbps for better internal communication.		
6	In case of scalability like horizontal scalability, the Service provider should ensure that additional requirement of network is provisioned automatically of same network segment.		
7	Service provider must ensure that the public network provisioned for cloud VMs is redundant at every points.		

Sr.	Description	Compliance Y/N	Remarks
8	Service provider must ensure that cloud VMs are accessible from TSECL private network if private links P2P/MPLS is used by TSECL.		
9	Service provider must ensure that there is console access to cloud VMs, if TSECL require to access it using IPSEC/SSL or any other type of VPN.		
10	Service provider should have provision of dedicated virtual links for data replication between their multiple data center in order to provide secure data replication for DR services.		
11	Service provider should ensure use of appropriate load balancers for network request distribution across multiple cloud VMs.		

1.8 Cloud Data Center Specifications: -

Sr.	Description	Compliance Y/N	Remarks
1	The data-center of Service provider must be within India only.		
2	All the physical servers, storage and other IT hardware from where cloud resources are provisioned for TSECL must be within Indian datacenters only.		
3	The datacenters should have adequate physical security in place.		
4	The datacenters of Service provider should be separated in different geolocation in different seismic zones and not on same fault lines. The primary and DR site datacenters should be located in different state / UT.		
5	The datacenters should conform to at least Tier-3 standards (certified under TIA942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards.		
6	CSP should be MeitY empaneled for all the services (i.e. Public, VPC and GCC service offerings) as per the GI Cloud (MeghRaj) initiative and should be STQC audited		
7	The CSP must be certified for ISO 27001, ISO 22301, ISO 27017 and ISO27018 (Year 2013 or above) and provide service assurance and effectiveness of Management compliant with ISO 20000 standards.		

1.9 Cloud Compatibility Requirement: -

Sr.	Compatibility	Compliance Y/N	Remark
1	Service provider must ensure that the virtual machine format is compatible with other cloud provider.		
2	TSECL should be able to export the virtual machine from Service provider cloud and use that anywhere i.e., in different Service provider.		
3	Service provider should provision to import cloud VM template from other cloud providers.		
4	Service provider should ensure connectivity to and from cloud resources of TSECL is allowed to/from other cloud service providers if required and approved by TSECL.		

1.10 Cloud Security Requirement: -

Sr.no	Description	Compliance Y/N	Remarks
1	Service provider should ensure there is multi-tenant environment and cloud virtual resources of TSECL are logically separated from others.		
2	Service provider should ensure that any OS provisioned as part of cloud virtual machine should be patched with latest security patch.		
3	In case, the Service provider provides some of the System Software as a Service for the project, Service provider is responsible for securing, monitoring, and maintaining the System and any supporting software.		
4	Service provider should implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage		
5	Service provider should deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.		
6	Service provider should give ability to create non-production environments and segregate (in a different VLAN) non-production environments from the production environment such that the users of the environments are in separate networks.		
7	Service provider should have built-in user-level controls and administrator logs for transparency and audit control.		
8	Service provider cloud platform should be protected by fully managed Intrusion detection system using signature, protocol, and anomaly based inspection thus providing network intrusion detection monitoring.		
9	Service provider would be responsible for proactive monitoring and blocking against cyberattacks and restoration of services in case of attacks.		

1.11 Virtual Machine Specifications: -

S.No.	Description	Compliance Y/N	Remarks
1	The Cloud virtual machine provided by Service provider should be provisioned on redundant physical infrastructure.		
2	The cloud virtual machines should be scalable in terms of RAM and CPU.		
3	TSECL should be able to provision cloud virtual machine of any operating system like Linux and Windows.		
4	Service provider should clearly define policies to handle data in transit and at rest.		
5	Without handover of entire data back to TSECL, Service provider should not delete any data at the end of contract period without consent from TSECL.		
6	Service provider should provide facility to make template from virtual machines.		

7	Service provider should enable to select configuration of cloud virtual machine-like custom RAM, CPU and disk.		
8	Service provider should make provision to add any virtual machine as part of scalable infrastructure.		
9	Service provider should have provision to live migration of virtual machine to another physical servers in case of any failure.		
10	Service provider should deliver cloud having method and system for detecting, in real time, resource requirements of a system in virtual environment and automatic scaling of resource parameters to compensate resource requirement in a system. The Virtual machine controller constantly measures resource utilization in the servers and virtual machines associated with it. If a resource requirement is detected with any virtual machine, the automatic resource scaling system detects the type of resource to be scaled and scales the selected resource. Further, the resource may be scaled up or scaled down, based on the requirements. Further, the scaled resource may be CPU, RAM, disk or any such resource. The proposed system helps to save space and power without compromising security, performance and accessibility		

1.12 Cloud Resource and Network Monitoring: -

S.No.	Description	Compliance Y/N	Remarks
1	Service provider should give provision to monitor the network traffic of cloud virtual machine.		
2	Service provider should offer provision to analyze of amount of data transferred of each cloud virtual machine.		
3	Service provider should provide network information of cloud virtual resources.		
4	Service provider should offer provision to monitor latency to cloud virtual devices from its datacenter or TSECL should be able to set monitoring of latency to cloud VMs from outside world.		
5	Service provider must offer provision to monitor network uptime of each cloud virtual machine.		
6	Service provider must make provision of resource utilization i.e. CPU graphs of each cloud virtual machine.		
7	Service provider must make provision of resource utilization graph i.e. RAM of each cloud virtual machine. There should be provision to set alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.		
8	Service provider must make provision of resource utilization graph i.e. disk of each cloud virtual machine. There should be graphs of each disk partition and email alerts should be sent if any threshold of disk partition utilization is reached.		
9	Service provider should give provision to monitor the uptime of cloud resources. The report should be in exportable form.		

S.No.	Description	Compliance Y/N	Remarks
10	Service provider must give provision to monitor the load of Linux/Windows servers and set threshold for alerts.		
11	Service provider should make provision to monitor the running process of Linux/Windows servers. This will help TSECL to take the snapshot of processes consuming resources.		
12	Service provider must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.		
13	Service provider must ensure that audit logs of scalability i.e. horizontal and vertical is maintained so that billing disputes can be addressed.		
14	Service provider must ensure that log of reaching thresholds used to trigger additional resources in auto provisioning are maintained.		
15	Service provider must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.		
16	Service provider should provide network information of cloud virtual resources.		
17	Service provider should offer provision to monitor latency to cloud virtual devices from its datacenter or TSECL should be able to set monitoring of latency to cloud VMs from outside world.		
18	Service provider must offer provision to monitor network uptime of each cloud virtual machine.		
19	Service provider must provide utilization reports for Internet bandwidth, load balancers etc.		

1.13 Application Performance Monitoring: -

a. Database Monitoring

Sr.no	Description	Compliance Y/N	Remarks
	a. Database monitoring:		
1	APM should be able to provide Overview of database server like Database details, version etc.		
2	APM should be able to provide host details which are connected to database Server		
3	APM should be able to provide session details of all active database sessions.		
4	Monitoring & management of network link proposed as part of this solution.		
5	APM should be able to provide server configuration details. (All configurations, Advanced Configurations, RECONFIGURE Configurations, Memory Configurations)		
6	Bandwidth utilization, latency, packet loss etc.		
7	APM should be able to provide Jobs and Backup Details, including the following:		
	i) Currently executing Jobs.		

Sr.no	Description	Compliance Y/N	Remarks
	ii) Job Steps Execution Info.		
	iii) Job Schedule Info.		
	iv) Recent Database Backup.		
	v) Back-Up within Past 24 Hours.		
8	APM should monitor and provide details on the following queries performance parameters:		
	i) Top Queries by CPU , Top Queries by I/O		
	ii) Top Waits by Waiting Tasks, Top Slow Running Queries		
	iii) Most Frequently Executed Queries, Most Blocked Queries		
	iv) Top Queries by Lowest Plan Reuse, Cost of Missing Indexes		
9	APM should provide to set following monitoring parameters for continuous monitoring:		
	i) Total Server Memory, SQL Cache Memory		
	ii) Optimizer Memory, Lock Memory		
	iii) Connection Memory, Target Server Memory		
	iv) Granted Workspace Memory, Buffer Cache Hit Ratio		
	v) Page Lookups/Sec, Pages Read/Sec		
	vi) Page Life Expectancy (ms)		
	vii) User Connections, Logins/Sec		
	viii) Logouts/Sec, Cache Hit Ratio		
	ix) Cache Count, Cache Pages		
	x) Lock Requests/Sec, Lock Wait/Sec		
	xi) Lock Timeout/Sec , Full Scans/Sec		
	xii) Range Scans/Sec, Probe Scans/Sec		
	xiii) Work Files Created/Sec, Worktables Created/Sec		
	xiv) Index Searches/Sec, Latch Waits/Sec		
	xv) Average Latch Wait Time, Batch Requests/Sec		
	xvi) SQL Compilations/Sec, SQL Recompilations/Sec		
	xvii) Auto-Param Attempts/sec, Failed Auto-Params /Sec		
	xviii) Safe Auto-Params/Sec, Unsafe Auto-Params/Sec		
	xix) Availability		

b. Web Server

Sr.no.	Description	Compliance Y/N	Remarks
1	APM should provide website details hosted on web server.		
2	APM should provide application details running on web server.		
3	Monitoring & management of network link proposed as part of this solution.		
4	Bandwidth utilization, latency, packet loss etc.		
5	APM should consist of the following monitoring parameters:		

Sr.no.	Description	Compliance Y/N	Remarks
	i) Site Status, Total Bytes Sent		
	ii) Bytes Sent/Sec, Total Bytes Received		
	iii) Bytes Received/Sec, Total Bytes Transferred		
	iv) Bytes Total/Sec, Total Files Sent		
	v) Files Sent/Sec, Total Files Received		
	vi) Files Received/Sec, Current Connections		
	vii) Maximum Connections, Total Connection Attempts		
	viii) Total Logon Attempts, Service Uptime		

c. Application/Web server

Sr.No	Description	Compliance Y/N	Remarks
1	APM should consist of the following monitoring parameters:		
	i) Memory Monitoring		
	ii) Web Applications and Deployments		
	iii) Connections, Transactions, Queries		
	iv) Web Metrics		
	v) Transactions		
	vi) Availability		
2	Monitoring & management of network link proposed as part of this solution.		
3	Bandwidth utilization, latency, packet loss etc.		

1.14 Web Application Firewall as a Service: -

Sr.no.	Description	Compliance Y/N	Remarks
1	Cloud platform should provide Web Application Filter for OWASP (Open Web Application Security Project) Top 10 protection		
2	Service provider WAF should be able to support multiple website security.		
3	Service provider WAF should be able to perform packet inspection on every request covering all 7 layers.		
4	Service provider WAF should be able to block invalidated requests.		
5	Service provider WAF should be able to block attacks before it is posted to website.		
6	Service provider WAF should have manual control over IP/Subnet. i.e., Allow or Deny IP/Subnet from accessing website.		
7	The attackers should receive custom response once they are blocked.		
8	Service provider must offer provision to customize response of vulnerable requests.		

Sr.no.	Description	Compliance Y/N	Remarks
9	Service provider WAF should be able to monitor attack incidents and simultaneously control the attacker IP.		
10	Service provider WAF should be able to Whitelist or Backlist IP/Subnet.		
11	Service provider WAF should be able to set a limit to maximum number of simultaneous requests to the web server & should drop requests if the number of requests exceed the threshold limit.		
12	The WAF should be able to set a limit to maximum number of simultaneous connections per IP. And should ban / block the IP if the threshold is violated.		
13	WAF should be able to set a limit to maximum file size, combined file size in bytes		
14	WAF should be able to limit allowed HTTP versions, request content type, restricted extensions & headers		
15	Service provider WAF should be able to limit maximum number of arguments, argument name, value, value total length etc.		
16	Should be able to BAN an IP for a customizable specified amount of time if the HTTP request is too large.		
17	Should be able to limit maximum size of request body entity in bytes		
18	The WAF should be able to close all the sessions of an IP if it is ban.		
19	Should be able to Ban IP on every sort of attack detected and the time span for ban should be customizable. There should be a custom response for Ban IP.		
20	The WAF access and security Dashboard should show a graphical representation of		
	A) For access report analysis purpose, the Dashboard should contain following information:		
	i) Number of hits by status code		
	ii) HTTP status code wise hits		
	iii) HTTP methods wise hits		
	iv) Client browser wise hits		
	v) Client Operating system wise hits		
	vi) Traffic (No. of hits) per URL		
	vii) Average bytes received per request		
	viii) Average bytes sent per request		
	ix) Average time elapsed per request		
	B) For security report analysis purpose, the Dashboard should contain following information:		
	i) Average score by status code		
	ii) Distribution of blocked requests		

Sr.no.	Description	Compliance Y/N	Remarks
	iii) Number of blocked requests		
	iv) OWASP Top 10 requests		
	v) Reputation tags		
	vi) IP list reputation		
	C) For network incoming and outgoing traffic captured by WAF packet filter dashboard should contain following information:		
	i) Number of packet hits		
	ii) Source IP, Destination IP wise hits		
	iii) Firewall actions (allow, deny) wise hits		
	iv) Requests per destination port wise hits		
21	WAF should support different policies for different web applications.		
22	Vendor to ensure 24x7x365 availability of WAF service.		
23	WAF should support different policies for different application section (different security zones within the app).		
24	WAF should support IP Reputation DB (DB including blacklisted IP Address, IP Address, Anonymous Proxy, Botnets, Windows Exploit etc.) along with Client Source IP address-based Security Policy and dynamic source IP blocking.		
25	WAF should enforce file upload control based on file type, size etc.		
26	WAF should detect known malicious users who are often responsible for automated and botnet attacks. Malicious users may include malicious IP addresses or anonymous proxy addresses.		
27	WAF should support detection only, blocking and transparent mode.		
28	WAF solution should be capable of handling IPV4 and IPV6 traffic.		
29	WAF solution should ensure compliance and advanced protection against industry standards such as OWASP Top 10 vulnerabilities etc.		
30	Vendor must monitor, manage & maintain the WAF solution on a 24x7 basis.		
31	WAF should provide a real-time dashboard with data such as top attacks view, traffic monitoring view, etc.		
32	WAF should provide role-based access control for the dashboard (role based multiple login accounts both primary and secondary to be provided).		
33	WAF should provide detailed reports for all web application attacks.		
34	WAF should be able to decrypt the SSL traffic to analyse the HTTP data and should be able to re-encrypt the SSL traffic.		
35	WAF should support SSL offloading.		
36	WAF should support body inspection, content injection, backend compression, validation of UTF8 Encoding, XML Inspection.		

Sr.no.	Description	Compliance Y/N	Remarks
37	WAF should block invalid BODY.		
38	WAF should log all transactions for auditing purpose.		
39	WAF should block desktop users User-Agent, crawlers User-Agent, suspicious User-Agent.		
40	WAF should have DOS and BF protection for all or specific URLs.		
41	WAF should have learning mode to create whitelist/blacklist rules and also block attack in learning mode.		
42	WAF should verify SSL certificate, certificate name, expiration and cipher suites. Also control over accepted TLS/SSL protocol, cipher order, CRL verification, HTTP public key pinning, OCSP stapling.		
43	WAF should allow to inject Request and Response headers for applications.		
44	WAF should support Content and URL rewriting policies.		
45	WAF should send proxy HTTP headers to backend, r rewrite cookie path, backend' s cookies encryption and override backend server HTTP errors.		
46	WAF should support force HTTP to HTTPS redirection.		
47	WAF should support URL specific rulesets and should allow/deny specific countries (GeoIP) for applications.		
48	WAF should have OS level firewall to PASS/BLOCK traffic inbound/outbound traffic		
49	WAF should allow to create custom rules for application.		
50	WAF should support Active-Active/Active-Passive failover.		

1.15 Vulnerability Monitoring and Assessment Scanning Tool: -

Sr.no.	Description	Compliance Y/N	Remarks
1	Monitoring of Web Applications including the corporate websites etc. and protect it from malicious mobile codes like computer viruses, worms, Trojan horses, spyware, adware, key-loggers and other malicious programs. The service should be non-Intrusive in nature and should be offered for at least 50 URLs.		
2	Malware Monitoring scanning should be performed on Daily basis. If any malware is injected into Web Applications, then immediate malware alert message is forwarded to the stakeholders. Application Audit and Vulnerability assessment on weekly basis to ascertain if any corrective action needs to be taken in application based on any observations found in the scanning.		
3	Should be able to detect malicious code injection/links, both known and unknown malware, Web-page tampering, various zero-day browser exploits etc.		

Sr.no.	Description	Compliance Y/N	Remarks
4	Should be able to identify the malware source, malware threat area and coverage, encoded Java Script and VB script and should not rely on pattern/signature-based technology.		
5	It should have minimal impact on traffic, server performance, networks etc. during deployment and operation		
6	Should be able to work in any network topology.		
7	Should be able to identify applications running on non-standard ports		
8	Should have configurable scan intervals (frequency), Configurable notification, alerting and reporting options, Configurable "whitelist" option for allowed links, Configurable scan schedules and on-demand scans.		
9	Should have Real-time instant alerting upon detection of malicious behavior (Email or SMS).		
10	Should have detailed remediation recommendation guidance including step by step instructions on how to address the threats captured.		
11	Should have On demand Vulnerability Scanning without user intervention		
12	Should Perform a targeted scan (i.e. check for a specific set of vulnerabilities or IP Addresses).		
13	Should be able to conduct vulnerability assessment for all operating systems and their versions including but not limited to : Windows, AIX, UNIX, Linux, Solaris servers etc.		
14	Should be able to perform authenticated and unauthenticated scans		
15	Should be able to detect weak password.		
16	Should be able to identify out-of-date software versions, applicable patches and system upgrades		
17	Should Flag the presence of any blacklisted software		
18	Should be able to perform On demand Application Audit for all types of websites including AJAX, WEB2.0, and obfuscated Java Script etc. and identifies vulnerabilities throughout the entire application, scanning the browser and server-side components.		
19	Should check regularly for Defacement Detection, websites changes and detect for possible defacement. Such daily defacement checks protect the brand, credibility and reputation of the bank.		
20	Should have a Executive Dashboard that provides a comprehensive synopsis of reported vulnerabilities and malware, remediation suggestions as well as several alert and support options in predefined report formats. It should have Role based access.		

Sr.no.	Description	Compliance Y/N	Remarks
21	Should be able to provide remediation information in the reports including links to patches etc.		
22	Should be able to produce a report listing all applications on a host or network, regardless of whether the application is vulnerable		
23	Should Include a library of potential vulnerabilities and rules which covers SANS (SANS Institute) top 20. This library should be customizable by administrator and changes to the same are to be traceable.		
24	Provide detailed report as spreadsheet, PDF and HTML format, customizable as per the requirement and comparable to previous assessment.		
25	Should be able to generate reports on trends in vulnerabilities on a particular asset.		
26	Should have Scan history and comparison provided in Scan Report.		
27	Should have banner grabbing feature which tries to discover web-applications in the domain.		
28	Should Support industry standard reporting including OWASP top 10 categories.		
29	Should support authenticated scanning with different authentication methods including		
	Form, HTTP basic, NTLM and digest.		
30	The web application vulnerability scanning module should be able to identify the following vulnerabilities but not limited to in the underlying application.		
	· XSS		
	· Form Validation		
	· Block Malformed content		
	· Back Doors		
	· Spoofing		
	· SQL injection		
	· Directory/path traversal		
	· Forceful browsing		
	· LDAP injection		
	· SSI injections		
	· XPath injection		
	· Sensitive information leakage		
31	Should support domain reputation in Google, SURBL, Malware Patrol, Clean-Mx, Phishtank		

Sr.no.	Description	Compliance Y/N	Remarks
32	Should be able to check mail server IP and check in multiple RBL repositories		
33	Should be able to scan SQL Injections for My SQL, MSSQL, PGSQL, Oracle databases.		
34	Should be able to scan Local file inclusion (LFI), Remote file inclusion (RFI) , XSS - Cross Site Scripting & Malware.		
35	The scanning should support\cover following		
	· Open ports scanning for Security Threats		
	· Banner detection, directory scanning & directory indexing.		
	· Full Path disclosure in the pages		
	· Password auto complete enabled fields		
	· Page defacement detection & view state decoder		
	· Password submission method		
	· Time based scanning		
	· Robust link crawler		
	· SSL Certificate checking		
	· Web Shell Locater & Web Shell Finder		
	· Reverse IP domain check		
36	Generate logs for scanner access and testing.		
37	Solution should be a tool based automated solution		
38	Solution should support scanning of static and dynamic links		
39	Solution should be independent of application platform		
40	Malware Monitoring scanning on hourly basis. If any malware is injected into Web Applications, then immediately malware alert message shall be forwarded to authority. Application Audit and Vulnerability assessment of weekly basis.		
41	It should be able to integrate with other security solutions (i.e. Security Information / Event Management, Patch Management, IDS, IPS, etc.)		
42	It should integrate with the existing / proposed WAF solution		
43	24*7 monitoring / scanning of web pages for real time detection of malware injection. No skipping of page scanning.		
44	The service provider should have the ability to provide/Create Users with various privilege levels (view only / View or take down certain incident types)		

1.16 Endpoint Security

S.No	Description	Compliance YES/NO	Remark
1	Endpoint solution should have capability of AV, Vulnerability detection, malware protection, HIPS, Firewall, Device control ,sandbox and data loss prevention with pre and post machine learning execution in a single agent		
2	Endpoint vulnerability protection should scan the machine and provide CVE number visibility.		
3	Behavior monitoring along with ransomware protection engine, ransomware engine should have feature to take backup of ransom ware encrypted files and restoring the same.		
4	Endpoint solution should have data loss prevention with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based.		
5	Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting.		
6	OEM must be in Leader's quadrant for any of last two published report of Gartner MQ for Endpoint Security Or OEM must be Leader in Forrester in any of last two published report for Endpoint Security.		
7	Contains broad coverage of pre-categorized applications that can be easily selected from application catalog (with regular updates).		
8	Features system lockdown to harden end-user systems by preventing new applications from being executed		
9	Dynamically adjusts security configuration based on the location of an endpoint.		
10	Organizes vulnerability assessments by Microsoft security bulletin numbers, CVE numbers, or other important information		
11	Solution must support CPU usage performance control during scanning -Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer i.e. High, Medium and low.		

1.17 Server workload Security

S.No	Description	Compliance YES/NO	Remark
1	The solution must provide a single platform for complete server protection over physical, virtual & cloud.		
2	Should provide layered defense against advanced attacks and shields against known vulnerabilities in web and enterprise applications and operating systems.		
3	Should prevent access to malicious web sites		
4	Should have the capability to Monitor inter-VM traffic and protects Hypervisor.		

5	Should protects a wide range of platforms: Windows, Linux, Solaris, HP- UX, AIX, VMware, Citrix, Hyper-V, and Amazon.		
6	Should provide self-defending servers; with multiple integrated modules below providing a line of defense at the server: firewall, Anti-Malware, HIPS etc.		
7	Solution should have state full Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring and Recommended scan in single module or an in single agent.		
8	Proposed solution must have a dashboard to display multiple information.		
9	Proposed solution must have a web-based management system for administrators to access using web browsers		
10	Management server should have centralized management for physical, virtual & cloud environment.		
11	Management console should provide Firewall Events to view activities on computers with the firewall enabled (typically includes dropped or logged packets).		
12	The solution should display exploits detected, either resulting in dropped traffic (Prevent Mode) or logging of events (Detect Mode).		
13	Management console should provide System Events to view a summary of security- related events, primarily for the Management server and also including Agents' system events. All administrative actions should be audited within the System Events.		
14	The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites.		
15	Solution should have feature of high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.		
16	Solution should be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.		
17	Solution should provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred.		
18	Solution should have out-of-the-box vulnerability protection for over 100		

	applications, including database, Web, email, and FTP services etc.		
19	Solution should include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits		
20	Solution should automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot.		
21	Solution should cover of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.) with fine-grained filtering (IP and MAC addresses, ports) and basic prevention of denial of service (DoS) attack		
22	Solution should be able to detect and protect from reconnaissance scans and solution should have zero-day threat protection		
23	Solution should be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes.		
24	Solution should provide virtual protection which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs/physical servers within minutes.		
25	The solution should support Application control, behavior monitoring & Ransomware protection.		
26	The solution should have the capability to integrate with proposed existing solution for Zero-day attack prevention.		
27	Solution should support at least Windows 10, Windows Server 2008, 2012, 2016, RHEL 32 bit and 64 bit, CentOS, Debian, Ubuntu, AIX, HP-UX, Oracle Linux, and SUSE.		
28	Provides out of the box compliance support for PCI & NIST and OEM should provide engineer (Direct from OEM) with at least 5 working days during implementation to perform audit on product and help out during implementation		
29	The solution must be certified to Common Criteria EAL 2+.		
30	Offered Solution should be in recommended list as per latest IDC report on Server Security		
31	Management Server should be hosted as a service in India so that no data goes outside India for threat analysis.		

1.18 Container Security

S.No	Description	Compliance YES/NO	Remark
1	The solution should be deployed as a minimal agent on the cloud workloads such as VMs, Conatiners and Serverless to provide asked security features to the workloads and a should provide a unified workload protection framework to protect cloud native applications across different environments such as cloud managed Kubernetes platform, self-operated Kubernetes platform, OpenShift and etc		
2	The solution must provide a defense-in-depth approach to protect the host-VMs, Containers and Serverless functions across their lifecycle by using continuous vulnerability management and runtime defense		
3	The solution should provide for grouping of the containers by Cluster		
4	The solution should support auto-upgrade support for agents deployed on host and container runtime environments		
5	The solution should be able to detect threat based on malicious behavior patterns of processes running in container and at host level		
6	The solution should provide runtime protection for container and host east-west traffic with IPS module		
7	The solution should detect anomalies in running workloads by co-relating various metrics and map the same with MITRE ATT&CK techniques		
8	The solution should be provided as a SaaS or on prem software tool with supoort for environment like VMs , Kubernetes -container in AWS/Azure/GCP cloud environemnts etc. It should provide flexibility of securing cloud native software stacks on Openshift, Kubernetes, and Tanzu container environment etc.		
9	Solution must support integration with various automation deployment tools like Ansible, Chef, AWS Systems manager etc.		
10	The solution must have Alerting integration with developer and operations tools like Jira, Slack, and other SIEM platforms		
11	Should perform continuous vulnerability management across all types of workloads such as VM, Container registry, Serverless and Code repository		

1.19 Managed Services: -

S.No	Managed Services	Compliance YES/NO	Remark
	a. Network and Security Management:		
1	Monitoring & management of network link proposed as part of this solution.		
2	Bandwidth utilization, latency, packet loss etc.		
3	Call logging and co-ordination with vendors for restoration of links, if need arises.		
4	Redesigning of network architecture as and when required by TSECL		
5	Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion protection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.		
6	Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately		
7	Ensure a well-designed access management process, ensuring security of physical and digital assets, data and network security, backup and recovery etc.		
8	Adding/ Changing network address translation rules of existing security policies on the firewall		
9	Diagnosis and resolving problems related to firewall, IDS /IPS.		
10	Managing configuration and security of Demilitarized Zone (DMZ) Alert / advise TSECL about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc.		
	b. Server Administration and Management:		
1	Administrative support for user registration, User ID creation, maintaining user profiles, granting user access, authorization, user password support, and administrative support for print, file, and directory services.		
2	Setting up and configuring servers and applications as per configuration documents/ guidelines provided by TSECL		
3	Installation/ re-installation of the server operating systems and operating system utilities		
4	OS Administration including troubleshooting, hardening, patch/ upgrades deployment, BIOS & firmware upgrade as and when required/ necessary for Windows, Linux or any other O.S proposed as part of this solution whether mentioned in the RFP or any new deployment in future.		

S.No	Managed Services	Compliance YES/NO	Remark
5	Ensure proper configuration of server parameters, operating systems administration, hardening and tuning		
6	Regular backup of servers as per the backup & restoration policies stated by TSECL from time to time		
7	Managing uptime of servers as per SLAs.		
8	Preparation/ updation of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening		

1.20 Database Support Services: -

S.No	Database Support Service	Compliance YES/NO	Remarks
1	Installation, configuration, maintenance of the database (Cluster & Standalone).		
2	Regular health checkup of databases.		
3	Regular monitoring of CPU & Memory utilization of database server, Alert log monitoring & configuration of the alerts for errors.		
4	Space monitoring for database table space, Index fragmentation monitoring and rebuilding.		
5	Performance tuning of Databases.		
6	Partition creation & management of database objects, Archiving of database objects on need basis.		
7	Patching, upgrade & backup activity and restoring the database backup as per defined interval.		
8	Schedule/review the various backup and alert jobs.		
9	Configuration, installation and maintenance of Automatic Storage Management (ASM), capacity planning/sizing estimation of the Database setup have to be taken care by the Bidder.		
10	Setup, maintain and monitor the 'Database replication' / Physical standby and Assess IT infrastructure up-gradation on need basis pertaining to databases.		
11	Tuning of high-cost SQLs and possible solution to application development team for tuning in order to achieve optimum database performance.		

1.21 Helpdesk Support from Cloud Service Provider: -

S.No	Helpdesk Support	Compliance YES/NO	Remarks
1	Service provider should provide flexibility of logging incident manually via windows GUI and web interface.		
2	The web interface console of the incident tracking system would allow viewing, updating, and closing of incident tickets		
3	Allow categorization on the type of incident being logged		

S.No	Helpdesk Support	Compliance YES/NO	Remarks
4	Provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels		
5	Provide audit logs and reports to track the updating of each incident ticket		
6	It should be able to log and escalate user-based requests.		
7	Service provider should allow ticket logging by email, chat or telephone.		

1.22 SIEM Service: -

Sr. No.	SIEM Description	Compliance YES/NO	Remarks
1	The solution should be able to handle a minimum of Avg 5.06 Eps / Device		
2	The solution should be scalable by adding additional receivers and still be managed through a single, unified security control panel.		
3	The solution should be capable of real time analysis and reporting.		
4	The platform should not require a separate RDBMS for log collection, web server or any kind of application software for its installation.		
5	The solution should be able to assign risk scores to your most valuable asset. The risk value could be assigned to a service, application, specific servers, a user, or a group. The solution should be able to assign and consider the asset criticality score before assigning the risk score.		
6	The relative risk of each activity should be calculated based on values assigned by the Asset Administrator.		
7	The activities should be separated by levels of risk for the company: very high, high, medium, low and very low.		
8	The SIEM receiver/log collection appliance must be an appliance-based solution and not a software based solution to store the data locally, if communication with centralized correlator is unavailable.		
9	The solution should be able to collect logs via the following ways as inbuilt into the solution: Syslog, OPSec, agent-less WMI, RDEP, SDEE, FTP, SCP, External Agents such as Adiscon.		
10	The solution should provide a data aggregation technique to summarize and reduce the number of events stored in the master database.		
11	The solution should provide a data store which is compressed via flexible aggregation logic.		
12	The data collected from the receiver should be forwarded in an encrypted manner to SIEM log storage.		
13	The solution should provide pre-defined report templates. The reports should also provide reports out of the box such as ISO 27002.		

Sr. No.	SIEM Description	Compliance YES/NO	Remarks
14	The solution should provide reports that should be customizable to meet the regulatory, legal, audit, standards and management requirements.		
15	The solution should also provide Audit and Operations based report, Native support for Incident management workflow.		
16	The solution should have single integrated facility for log investigation, incident management etc. with a search facility to search the collected raw log data for specific events or data.		
17	A well-defined architecture along with pre and post installation document need to be shared by the bidder.		
18	The solution should have a scalable architecture, catering multi-tier support and distributed deployment.		
19	The solution should support collection of events/logs and network flows from distributed environment(s).		
20	The solution should correlate security/network events to enable the SOC to quickly prioritize it's response to help ensure effective incident handling.		
21	The solution should integrate asset information in SIEM such as categorization, criticality and business profiling and use the same attributes for correlation and incident management.		
22	The solution should provide remediation guidance for identified security incident:		
23	a) Solution should be able to specify the response procedure (by choosing from the SOPs) to be used in incident analysis/remediation.		
24	The solution should facilitate best practices configuration to be effectively managed in a multi-vendor and heterogeneous information systems environment.		
25	The solution should provide capability to discover similar patterns of access, communication etc. occurring from time to time, for example, slow and low attack.		
26	The solution should perform regular (at least twice a year) health check and fine tuning of SIEM solution and should submit a report.		
27	The solution should share the list of out of the box supported devices/log types.		
28	The solution should support hierarchical structures for distributed environments. The solution should have capability for correlation of events generated from multiple SIEM(s) at different location in single management console.		
29	The event correlation on SIEM should be in real time and any delay in the receiving of the events by SIEM is not acceptable.		
30	The solution should support internal communication across SIEM-components via well-defined secured channel. UDP or similar ports should not be used.		
31	Event dropping/caching by SIEM solution is not acceptable and same should be reported and corrected immediately.		

Sr. No.	SIEM Description	Compliance YES/NO	Remarks
32	The solution should be able to facilitate customized dashboard creation, supporting dynamic display of events graphically.		
33	The solution should be able to capture all the fields of the information in the raw logs.		
34	The solution should support storage of raw logs for forensic analysis.		
35	The solution should be able to integrate logs from new devices into existing collectors without affecting the existing SIEM processes.		
36	The solution should have capability of displaying of filtered events based on event priority, event start time, end time, attacker address, target address etc.		
37	The solution should support configurable data retention policy based on organization requirement.		
38	The solution should provide tiered storage strategy comprising of online data, online archival, offline archival and restoration of data. Please elaborate on log management methodology proposed.		
39	The solution should compress the logs by at least 70% or more at the time of archiving.		
40	The solution should have capability for log purging and retrieval of logs from offline storage.		
41	Solution should be capable of replicating logs in Synchronous as well as Asynchronous mode for replication from Primary site to DR site.		
42	The solution should provide proactive alerting on log collection failures so that any potential loss of events and audit data can be minimized or mitigated.		
43	The solution should provide a mechanism (in both graphic and table format) to show which devices and applications are being monitored and determine if a continuous set of collected logs exist for those devices and applications.		
44	The solution should support automated scheduled archiving functionality into file system.		
45	The solution should support normalization of real time events.		
46	The solution should provide a facility for logging events with category information to enable device independent analysis.		
47	The platform should be supplied on Hardened OS embedded in Hardware / Virtual Appliance. The storage configuration should offer a RAID configuration to allow for protection from disk failure.		
48	The platform should have High Availability Configuration of necessary SIEM components to ensure there is no single point of failure. Please describe the architecture proposed to meet this requirement.		
49	By default at the time of storage, solution should not filter any events. However, solution should have the capability of filtering events during the course of correlation and report generation.		

Sr. No.	SIEM Description	Compliance YES/NO	Remarks
50	The solution should ensure the integrity of logs. Compliance to regulations should be there with tamper-proof log archival.		
51	The solution should be able to continue to collect logs during backup, de-fragmentation and other management scenarios.		
52	The solution should support collection of logs from all the devices quoted in RFP.		
53	The collection devices should support collection of logs via the following but not limited methods:		
54	1. Syslog over UDP / TCP		
55	2. SNMP		
56	3. ODBC (to pull events from a remote database)		
57	4. FTP (to pull a flat file of events from a remote device that can't directly write to the network)		
58	5. Windows Event Logging Protocol		
59	7. NetBIOS		
60	The solution should allow a wizard / GUI based interface for rules (including correlation rules) creation as per the customized requirements. The rules should support logical operators for specifying various conditions in rules.		
61	The solution should support all standard IT infrastructure including Networking & Security systems, OS, RDBMS, Middleware, Web servers, Enterprise Management System, LDAP, Internet Gateway, Antivirus, and Enterprise Messaging System, Data loss prevention (DLP) etc.		
62	The solution should have provision for integration of the following:		
63	d) Inclusion of "Application context".		
64	Solution should have license for minimum 10 users for SIEM administration.		
65	The solution should have the ability to define various roles for SIEM administration, including but not limited to: Operator, Analyst, SOC Manager etc. for all SIEM components.		
66	The solution should support SIEM management process using a web-based solution.		
67	The solution should support the following co- relation:		
68	Statistical Threat Analysis - To detect anomalies.		
69	Susceptibility Correlation - Raises visibility of threats against susceptible hosts.		
70	Vulnerability Correlation - Mapping of specific detected threats to specific / known vulnerabilities		
71	Rules based Correlation - The solution should allow creating rules that can take multiple scenarios like and create alert based on scenarios.		
72	Solution should have capability to correlate based on the threat intelligence for malicious domains, proxy networks, known bad IP's and hosts.		

Sr. No.	SIEM Description	Compliance YES/NO	Remarks
73	The solution should provide ready to use rules for alerting on threats e.g., failed login attempts, account changes and expirations, port scans, suspicious file names, default usernames and passwords, High bandwidth usage by IP, privilege escalations, configuration changes, traffic to non-standard ports, URL blocked, accounts deleted and disabled, intrusions detected etc.		
74	The solution should support the following types of correlation conditions on log data:		
75	a) One event followed by another event		
76	b) Grouping, aggregating, sorting, filtering, and merging of events.		
77	c) Average, count, minimum, maximum threshold etc.		
78	Solution should provide threat scoring based on:		
79	a) Host, network, priority for both source		
80	& Destination		
81	b) Real-time threat, event frequency, attack level etc.		
82	The solution should correlate and provide statistical anomaly detection with visual drill down data mining capabilities.		
83	The solution should have the capability to send notification messages and alerts through email, SMS, etc.		
84	The solution should support RADIUS and LDAP / Active Directory for Authentication.		
85	The solution should provide highest level of enterprise support directly from OEM.		
86	The solution should provide a single point of contact directly from OEM for all support reported OEM.		
87	The solution should ensure continuous training and best practice updates for onsite team from its backend resources.		
88	Solution should support log integration for IPv4 as well as for IPv6.		
89	Solution should provide inbuilt dashboard for monitoring the health status of all the SIEM components, data insert/retrieval time, resource utilization details etc.		
90	Solution should support at least 100 default correlation rules for detection of network threats and attacks. The performance of the solution should not be affected with all rules enabled.		
91	The central management console/ Enterprise Security managers/receivers should be in high availability.		
92	24/7 extensive monitoring of the cloud services and prompt responses to attacks and security incidents		
93	Recording and analysing data sources (e.g. system status, failed authentication attempts, etc.)		
94	24/7 contactable security incident handling and troubleshooting team with the authority to act		

Sr. No.	SIEM Description	Compliance YES/NO	Remarks
95	Obligations to notify the customer about security incidents or provide information about security incidents potentially affecting the customer		
96	Provision of relevant log data in a suitable form		
97	Logging and monitoring of administrator activities		

8.3.2. General Terms & Conditions

The aspect of reliability, availability and serviceability features as primary DC & DR Site are meant for running mission critical applications. While selecting the entire DC & DR Platform the care should be taken so that the selected Infrastructure should support the scalability, availability & performance.

i. The uptime required for entire GCC Infrastructure is 99.9%.
ii. The servers need to be certified for ERP requirement as mentioned in the ERP landscape.
iii. Detailed Specification & detailed BoM has to be shared by bidder.
iv. Appropriate Security solutions such as vFirewall/UTM, IPS/IDS/Anti-DDoS/VPN, software along with licenses for number of users / installed capacity, anti-virus applications etc. should be provided with the systems.
v. Appropriate network and data security solution should be designed for securing TSECL‟s application and data, minimum requirements are mentioned in the respective technical specifications, however, bidder can propose most optimum solution to secure entire solution, applications & data and provide secure access to TSECL‟s users over different links including Internet link considering Cert-In & NCIIPC – Critical Sector Guidelines
vi. Additional resources during failover with necessary Infrastructure, management software and licenses should be part of the solution
vii. CPU proposed should be as per ERP at 65% utilization.
viii. DR Drill has to be carried twice in a year.
ix. Compute and Storage of only Production landscape (without High Availability) of DC to be considered at DR.
x. Carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution.
xi. The Service Provider shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down.
xii. Manage the instances of storage, compute instances, and network environments. This includes department-owned & installed operating systems and other system software that are outside of the authorization boundary of the CSP. Service Provider is also responsible for managing specific controls relating to shared touch points within the security authorization boundary, such as establishing customized security control solutions.
xiii. Router for Point. to Point. link termination between DC & DR
xiv. Network Switch can be shared or dedicated.
xv. Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
xvi. Additional resources during failover with necessary Infrastructure, management software and licenses should be part of the solution.
xvii. All the proposed hardware, software and support part codes (if applicable) needs to be provided along with technical bid and commercial bid.

xviii. Furthermore, any other item required for the overall integration and functioning of the Data Centre, though not covered in the detailed specification, bill of materials, shall be within the scope of the bidder and should be included in the Solution.
xix. The bidder shall also provide all required equipment which may not be specifically stated in the RFP but are required to meet the intent of ensuring completeness, maintainability and reliability to support to run the application smoothly.
xx. Any non-compliance to above clauses & technical specifications will result in direct disqualification of the bid.
xxi. The CSP should ensure that the data should not leave the boundaries of the country and data residing with CSP and should not be accessed by any entity outside the control of Purchaser.
xxii. The CSP shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of the TSECL.
xxiii. Migration of the Application Suite from the existing infrastructure to the cloud infrastructure. The migration shall also include the migration of underlying data & files from the current database(s) / storage into the database(s) / storage on the cloud.
xxiv. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with TSECL.
xxv. In case of end of agreement, the bidder shall be responsible for providing the tools for import / export of VMs & content and TSECL shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition.
xxvi. Once the end of agreement and exit process is completed, Bidder to remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of TSECL as per stipulations and shall ensure that the data cannot be forensically recovered.
xxvii. At the end of the agreement, TSECL will ensure that all the storage blocks or multiple copies of data if any are unallocated or zeroed out by the bidder so that data cannot be recovered.
xxviii. Cloud service shall offer SSD backed storage and shall support High IOPS. CSP should deliver minimum 5000 IOPS per TB for OLTP load. The IOPS for NON OLTP load should be minimum 2000 per TB.
xxix. Bidder should provide Burstable internet bandwidth as per customer ask within 8Hours of SLA.
xxx. Bidder should meet/comply the following technical specifications failing which bidder will be rejected and its financial bid will not be opened.

8.3.1. Server Specification for Cloud Environment

INSTANCE TYPE	SPECIFICATION
Production	
Outbound Data	500 GB per month
FTP Storage	500 GB per month - Standard SSD
Managed DB - Postgres	16 vCPU with 300 GB storage per month - 99.9% availability
Load Balancer	Load Balancer with 5 rules per month
Virtual Machine - Web Server	16 vCPU/64 GB RAM - Windows Server 2019 or higher, Data Disk - 250 GB SSD per month - 99.9% availability
SIT	
Outbound Data	100 GB per month

FTP Storage	50 GB per month - Standard SSD
Managed DB - Postgres	4 vCPU with 30 GB storage per month - 99.9% availability
Load Balancer	Load Balancer with 5 rules per month
Virtual Machine - Web Server	4 vCPU/16 GB RAM - Windows Server 2019 or higher, Data Disk - 128 GB SSD per month - 99.9% availability
UAT	
Outbound Data	100 GB per month
FTP Storage	50 GB per month - Standard SSD
Managed DB - Postgres	4 vCPU with 30 GB storage per month - 99.9% availability
Load Balancer	Load Balancer with 5 rules per month
Virtual Machine - Web Server	4 vCPU/16 GB RAM - Windows Server 2019 or higher, Data Disk - 128 GB SSD per month - 99.9% availability
Dev	
Outbound Data	100 GB per month
FTP Storage	50 GB per month - Standard SSD
Managed DB - Postgres	4 vCPU with 30 GB storage per month - 99.9% availability
Load Balancer	Load Balancer with 5 rules per month
Virtual Machine - Web Server	4 vCPU/16 GB RAM - Windows Server 2019 or higher, Data Disk - 128 GB SSD per month - 99.9% availability
Security & Common Components for all environments	
Firewall	Network firewall with 2 Gbps throughput and support for 20 endpoints per firewall per month for all environments
DDoS & EDR	For all VM and Storage for all environments - per month
Web Application Firewall	Web Application Firewall - throughput of 20 Mbps with HTTP/S support and protection of upto 10 separate application VM/ACL, upto 10 rules each for all environments
Network	DNS Services - 2 External, 5 internal
Network	Connectivity between Cloud DC & DR - Atleast 100 Mbps per month
Network	Bandwidth - inbound per 100 GB

Network	Bandwidth - outbound per 100 GB
Network	Global Load Balancer with 5 TB data transfer per month
Network	Virtual Network/ Nat Gateway within DC to create zones - per 1 TB
Network	Virtual Network/ Nat Gateway DC-DR - per 100 GB
Network	Static IP Addresses - 5 per month
Monitoring	Monitoring and observability service - cost per month No. of metrics - 20 Logs Standard Logs - Data Ingested - 1 GB per day Analysis Logs - Data ingested - 1 GB per day Retention - 30 days
Monitoring	Network Monitor - 50 GB logs per month
Monitoring	Cloud Native SIEM service - cost per month Standard Logs - Data Ingested - 1 GB per day Standard Logs - Data Analysed - 1 GB per day
Monitoring	Bastion as a service - 1 unit - 730 hrs for RDP/SSH per month
DC-DR Replication	DC - DR Replication - per VM
Backup	VM backup with upto 500 GB disk
Backup	Disk Backup per TB
Backup	Disk snapshot per TB

9. Mandatory Forms

9.1. Bid Submission & Declaration Form

(To be submitted on the letter head of the bidder)

Ref: _____ Date: _____

To
The AGM (DP&C)
Corporate Office,
Tripura State Electricity Corporation Ltd.,
Bidyut Bhaban, Banamalipur,
Agartala, Tripura

Subject: Submission of Technical Bid for Award of Work "Selection of Cloud Service Provider/Managed Service Provider for hosting the ERP system in TSECL"

Dear Sir/Madam:

1. We the undersigned bidder/(s), having read and examined in details the specifications and other documents of the subject tender no. _____ dated _____, do hereby propose to execute the job as per specification as set forth in your Bid documents.
2. The prices of all items stated in the bid are firm during the entire period of job and not subject to any price adjusted as per in line with the bidding documents. All prices and other terms & conditions of this proposal are valid for a period of 180 (one hundred eighty) days from the date of opening of bid. We further declare that prices stated in our proposal are in accordance with the RFP.
3. We confirm that our bid prices include applicable GST.
4. We declare that items shall be executed strictly in accordance with the specifications and documents irrespective of whatever has been stated to the contrary anywhere else in our proposal. Further, we agree that additional conditions, deviations, if any, found in the proposal documents other than those stated in our deviation schedule, save that pertaining to any rebates offered shall not be given effect to.
5. If this proposal is accepted by you, we agree to provide services and complete the entire work, in accordance with schedule indicated in the proposal. We fully understand that the work completion schedule stipulated in the proposal is the essence of the job, if awarded.
6. We further agree that if our proposal is accepted, we shall provide a Performance Bank Guarantee of the value equivalent to ten percent (10%) of the Order value as stipulated in Price Bid.
7. We agree that TSECL reserves the right to accept in full/part or reject any or all the bids Yours Sincerely,

Dated, this .day of 2021

Thanking you, we remain,

Yours faithfully

Signature_____

Name in _____ full

Designation_____

Signature & Authorized Verified by

Name & Designation

Full Signature & Stamp

9.2. Bidder's Authorization Certificate

To
The AGM (DP&C)
Corporate Office,
Tripura State Electricity Corporation Ltd.,
Bidyut Bhaban, Banamalipur,
Agartala, Tripura

< Name>, <Designation> is hereby authorized to sign relevant documents on behalf of the company <bidder name>, in dealing with Tender of reference Tender No. tender no. _____ dated _____. He is also authorized to attend meetings & submit technical and commercial information as may be required by you in the course of processing above said tender.

Yours Sincerely,

Authorized Signature [In full and initials]	:……..
Name and Title of Signatory	:……..
Name of Firm:	:……..
Business Address	:……..
Bidder's Seal	
Place: ……..	Date: ……

9.3. Undertaking regarding debarment and/or blacklisting

I, _____ (Name of the Authorized person) presently working in the capacity of ……..(designation) and I have been duly authorized by ……(bidder name) a Company incorporated under the provisions of the Indian Companies Act 2013 /Limited Liability Partnership Act 2008, having its Registered office/ Corporate Office / at _____ to furnish the aforesaid undertaking against the specific requirement as specified in Tender No. _____ dated _____ and accordingly, I, on behalf of …….. (name of the bidder) hereby solemnly declare & affirm as under: -

That to the best of our knowledge and as per records available with the Company, _____ (Name of the bidder) have not been blacklisted / debarred / disqualified by any Govt. of India or any of its agencies, any State Govt. or any of its agencies, State or Central PSUs etc. during the last 5 years till the date of submission of Bid

Signature of Company Secretary/Authorized Key Managerial Personnel (KMP) of the Bidder's organization [In full and initials]	:……..
Name and Title of Signatory	:……..

10. Bidding Forms

10.1. Non-Disclosure Agreement

I, _____, on behalf of the _____(Name of Company), acknowledge that the information received or generated, directly or indirectly, while working with TSECL on contract is confidential and that the nature of the business of the TSECL is such that the following conditions are reasonable, and therefore:

I warrant and agree as follows:

I, or any other personnel employed or engaged by our company, agree not to disclose, directly or indirectly, any information related to the TSECL. Without restricting the generality of the foregoing, it is agreed that we will not disclose such information consisting but not necessarily limited to:

- **Technical information:** Methods, processes, formulae, compositions, systems, techniques, inventions, computer programs/data/configuration and research projects.
- **Business information:** Project schedules, pricing data, estimates, financial or marketing data.

On conclusion of contract, I, or any other personnel employed or engaged by our company shall return to TSECL all documents and property of TSECL, including but not necessarily limited to: drawings, blueprints, reports, manuals, computer programs/data/configuration, and all other materials and all copies thereof relating in any way to TSECL, or in any way obtained by me during the course of contract. I further agree that I, or any others employed or engaged by our company shall not retain copies, notes or abstracts of the foregoing.

This obligation of confidence shall continue after the conclusion of the contract also. Non-Disclosure Agreement is for 2 years from the date of contract closure.

I agree that this agreement shall be governed by and construed in accordance with the laws of country.

I enter into this agreement totally voluntarily, with full knowledge of its meaning, and without duress.

Dated at _____, this _____day of, 2019.

Authorized Signature [In full and initials]	:……..
Name and Title of Signatory	:……..
Name of Firm:	:……..
Business Address	:……..
Bidder's Seal	
Place: ……..	Date: ……

10.2. Pre-bid query format

Bidders requiring specific points of clarification may communicate (in Writing) with the Purchaser during the specified period using the following format:

Date: Bid Number: _____ Bidder Name:			
Sr. No.	Bidding document Reference (Section No./ Clause No. Page No.)	Content of Bidding document requiring clarification	Points of clarification required

Authorized Signature [In full and initials] :……..

Name and Title of Signatory :……..

Name of Firm: :……..

Business Address :……..

Bidder's Seal

Place: …….. Date: ……

10.3. Format for Deviations/Assumptions

To
Additional General Manager (DP&C)
Tripura State Electricity Corporation Ltd.,
Bidyut Bhawan, Banamalipur,
Agartala -799001.

Bid Number:					
S. No.	Bidding Document Reference (Section No. / Clause No. Page	Content of Bidding document	Deviation / Assumption	Financial Impact	Scope Impact

Note: In case of no deviation/assumption, bidder shall mention "Nil" in the above format.

Certificate:

We confirm that,

i. Only the above-mentioned deviations and/or assumptions may be considered.
ii. The Purchase is not bound to accept any of the above-mentioned deviation and/or assumption and may reject any or all without giving any reason thereof.
iii. Except the above-mentioned non-material deviations and/or assumptions, subject to the approval and acceptance by the Purchaser, the entire work shall be performed as per the bid requirements

Authorized Signature [In full and initials] :……..

Name and Title of Signatory :……..

Name of Firm: :……..

Business Address :……..

Bidder's Seal

Place: …….. Date: ……

10.4. Bidder's Financial Capabilities

The Details may be submitted in the following format
Bidder's Legal Name :_____ Date :_____

Information from Balance Sheet					
Sr. No.	Particulars	FY 2017-18 (Amount in INR)	FY 2018-19 (Amount in INR)	FY2019-20 (Amount in INR)	Enclose Documents
1	Total Assets				
2	Total Liabilities				
3	Net Worth (1-2)				
Information from Profit & Loss Statement					
7	Total Turnover (in INR)				
8	Average Turnover for 3 years				

Note:

Attached are copies of financial statement (Balance Sheet including all related notes, and income statements) for the years required above, complying with the following conditions:

- All such documents reflect the financial information of the bidder and not sister or parent companies
- Historic financial statement must be audited by the Statutory Auditor
- Historic financial statement must be complete, including notes to the financial statement.
- Historic financial statement must correspond to accounting periods already completed and audited (no statement for partial period shall be requested or accepted)

Seal & Sign of Statutory Auditor or Chartered Accountant	
Name of the Audit Firm:	
Firm Reg. Number.	

Date:

(Signature, name and designation of the authorised signatory)

10.5. Details of Bidder's project experience

Sr. No.	Project Details	Client Name & Sector	Project Start Date	Project Go-Live Date	Current Status	Page reference
1						
2						

10.6. BoQ

DC BOQ

Table 1
Production (PROD) and Development (DEV) Environment Server Specification

VM Name	vCPU	RAM (GB)	Storage (GB)	Storage Type	SAS Add on Storage (GB)	Qty (VM)	Instance
NAT INSTANCE (WEB Server)	2	8	10	SAS		1	PROD
FTP Storage					500	1	PROD
RDP HOST	2	1	30	SAS		1	PROD
RDS for PostgreSQL (DB Server)	16	64	300	SSD		2	PROD
Virtual Machine (App Server)	16	64	200	SAS		2	PROD
NAT INSTANCE (WEB Server)	2	4	10	SAS		1	DEV
FTP Storage					50	1	DEV
RDS for PostgreSQL (DB Server)	8	32	30	SSD		1	DEV
Virtual Machine (App Server)	4	16	50			1	DEV

Table 2

SIT and UAT Environment Server Specification

VM Name	vCPU	RAM (GB)	Storage (GB)	Storage Type	SAS Add On Storage (GB)	Qty(VM)	Instance
NAT INSTANCE (WEB Server)	2	4	10	SAS		1	SIT
FTP Storage					50	1	SIT
RDS for PostgreSQL (DB Server)	8	32	30	SSD		1	SIT
Virtual Machine (App Server)	4	16	50	SAS		1	SIT
NAT INSTANCE (WEB Server)	2	4	10	SAS		1	UAT
FTP Storage					50	1	UAT
RDS for PostgreSQL (DB Server)	8	32	30	SSD		1	UAT
Virtual Machine (App Server)	4	16	50	SAS		1	UAT

Table 3

Network Component				
Public IP's	**Private IP's**	**Location & Destination**	**Bandwidth Type**	**Bandwidth (Mbps)**
1	15	Internet	Dedicated	10

Component	Type	Qty
Network Port	WAN & LAN Network Port	2
Dedicated Firewall	VDOM with 1 S2S, 30 RA VPN Clients	1

Table 4

Software Licenses		
Software Type	**Product Name/Type**	**QTY**
OS	Windows Server 2019 Standard	6
OS	CentOS 7 (Freeware)	9
DB	PostgreSQL (Freeware)	5
DDOS Service	AntiDDOS - per 5Gbps protection	1
WAF Service	Basic WAF per subdomain - Protection against OWASP attacks (ex. Xss, injections), application and parameter/HPP Tampering	1
Load Balancer Service	Application Load Balancer (1 VIP) 2 Gbps throughput	1
Anti-virus	Antimalware	6
Backup	DB Level	4

DR BOQ

Table 1

Production (PROD) Environment Server Specification

VM Name	vCPU	RAM (GB)	Storage (GB)	Storage Type	SAS Add on Storage (GB)	Qty (VM)	Instance
NAT INSTANCE (WEB Server)	2	8	10	SAS		1	PROD
FTP Storage					500	1	PROD
RDP HOST	2	1	30	SAS		1	PROD
RDS for PostgreSQL (DB Server)	16	64	300	SSD		1	PROD
Virtual Machine (App Server)	16	64	200	SAS		1	PROD

Table 2

Network Component				
Public IP's	**Private IP's**	**Location & Destination**	**Bandwidth Type**	**Bandwidth (Mbps)**
1	15	Internet	Dedicated	10

Component	Type	Qty
Network Port	WAN & LAN Network Port	2
Dedicated Firewall	VDOM with 1 S2S, 30 RA VPN Clients	1

Table 3

Software Licenses		
Software Type	**Product Name/Type**	**QTY**
OS	Windows Server 2019 Standard	2
OS	CentOS 7 (Freeware)	2
DB	PostgreSQL (Freeware)	1
DDOS Service	AntiDDOS - per 5Gbps protection	1
WAF Service	Basic WAF per subdomain - Protection against OWASP attacks (ex. Xss, injections), application and parameter/HPP Tampering	1
Anti-virus	Antimalware	2
Backup	DB Level	1

11. Contract Forms

11.1. Format for BG against Performance Guarantee / Security Deposit

(To be stamped in accordance with stamp Act)

Ref. …….. Bank Guarantee No. ……

Date ……

To
Tripura State Electricity Corporation Limited
Bidyut Bhavan, North Banamalipur,
Agartala – 799001,
West Tripura.

Dear Sir,

In consideration of Tripura State Electricity Corporation Limited (hereinafter referred to as the 'Owner', which expression shall unless repugnant to the contest or meaning thereof include its successors, administrators and assigns) having awarded to M/s …….. with its registered / Head office at ……..(hereinafter referred to as 'Contractor' which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators, executors and assigns), a Contract by issued of Owner's Letter of Award No…….. dated…….. and the same having been acknowledged by the Contractor, resulting in a Contract bearing No. ……dated ……..valued at ……for ……(scope of contract) and the Contactor having agreed to provide a Contract Performance Guarantee for the faithful performance of the entire Contract equivalent to ……being (%) per cent) of the said value of the Contract to the Owner.

We,…… (Name & Address) having its Head Office at……..(hereinafter referred to as the 'Bank', which expression shall, unless repugnant to the context or meaning thereof, include its successors, administrators , executors and assigns) do hereby guarantee and undertake to pay the Owner, on demand any or all monies payable by the Contractor to the extent of ……..as aforesaid at any time up to …… ** (see in note below) …….. (days/month/year) without any demur, reservation, contest, recourse or protest and/or without any reference to the Contractor.

Any such demand made by the Owner on the bank shall be conclusive and binding notwithstanding any difference between the Owner and the Contractor or any dispute pending before any Court, Tribunal, Arbitrator or any other authority. The Bank undertakes not to revoke this guarantee during

its currency without previous consent of the Owner and further agrees that the guarantee herein contained shall continue to be enforceable till the Owner discharges this guarantee.

The Owner shall have the fullest liberty without affecting in any way the liability of the Bank under the guarantee, from time to time to extend the time for performance or the Contract by the Contractor. The Owner shall have the fullest liberty, without affecting this guarantee, to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the Contractor, and to exercise the same at any time in any manner, and either to enforce or to for bear to enforce any covenants, contained or implied, in the Contact between the Owner and the Contractor or any other course or remedy or security available to the Owner. The Bank shall not be released to its obligations under these presents by any exercise by the Owner of its liberty with reference to the matters aforesaid or any of them or by reason of any other act of omission or commission on the part of the Owner or any other indulgences shown by the Owner or by any other matter or thing what so ever which under law would, but for this provision have the effect of relieving the Bank.

The bank also agrees that the Owner at its option shall be entitled to enforce this guarantee against the Bank as a principal debtor, in the first instance without proceeding against the Contractor and not withstanding any security or other guarantee the Owner may have in relation to the Contactor's liabilities.

Notwithstanding anything contained herein above our liability under this guarantee is restricted to ……..and it shall remain in force upto and including ……..and shall be extended from time to time for such period (not exceeding one year), as may be desired M/s ……..on whose behalf this guarantee has been given.

Dated this …….. day of ……200…….. At …….

WITNESS

…… ……

(Signature) (Signature)

…… ……

(Name) (Name)

…… ……

(Official Address) (Official Address)

Attorney as per Power

Of Attorney No. ……..

Date ……..

NOTES:

- The sum shall be 'three per cent (3 %)' of the Contract Price.
- The claim date will be after the actual delivery period of 45 (forty-five) months plus a grace period of 3 (three) months making it a total of 48 (forty-eight) months.
- The Stamp Papers of appropriate value shall be purchased in the name of issuing Bank.

11.2. Draft Contract Agreement

APPENDIX-1 AGREEMENT

THIS AGREEMENT is made on this _____, between the **Tripura State Electricity Corporation Limited** (hereinafter called **"THE PURCHASER / TSECL"**), of the one part, and **_____** having its Registered Office at '_____' (hereinafter called **"THE Implementation Partner/ IP"**), of the other part:

AND WHERAS the Purchaser invited bids for Related Services, viz., Engagement of Implementation Partner for Supply, Installation, Implementation, Configuration and Integration of ERP system in TSECL of **Rs. _____ (_____)** including GST as applicable (hereinafter Called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Contract referred to.

2. The following documents (collectively referred to as "Contract Documents") shall be deemed to form and be read and construed as part of this Agreement, viz.:

   i. **Section I:** LOA award of contract vide no. _____ dated _____ 2021;

   ii. **SECTION II:** Request for Proposal issued vide Notification No. _____ dated _____ (Complete Bid Documents comprising of Terms & Condition, Instruction to the bidder, Scope of Work etc.);

   iii. **Section III:** Contract Forms/Performance Security Bank Guarantee.

   iv. **Section IV:** Proposal submitted by the Implementation Partner in response to the RfP mention in Sr. No. ii.

   v. **Section V:** Acceptance of purchaser's notification.

In the event of any discrepancy or inconsistency within the Contract documents, then the documents shall prevail in the order listed above.

3. In consideration of the payments to be made by the Purchaser to the Implementation Partner as indicated in this Agreement, the Implementation Partner hereby covenants with the Purchaser to provide the Related Services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Purchaser hereby covenants to pay the Implementation Partner in consideration of the provision of the services provided as per the RfP and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of **INDIA** on the day, month and year indicated above.

Signed by _____

(Authorized **TSECL** official)

Signed by _____

(For the Supplier)

_____

12. Bid Check List*

Sr. No.	Requirement	Submitted (Page No.)	Not Submitted	Remarks
1.	Copy of signed Tender document and subsequent amendments (if any)			
2.	Self-attested photocopy of valid Registration/ Incorporation Certificate - (Clause 21.5)			
3.	NIT document – Corrigendum, if published (ITB Clause 21.5)			
4.	Financial Documents (As mentioned in ITB Clause 21.5)			
5.	Miscellaneous Documents, if applicable (As mentioned in ITB Clause 21.5)			
6.	Self-attested photocopy of PAN card (ITB Clause 21.5)			
7.	Self-attested photocopy of GST registration Certificate (ITB Clause 21.5)			
8.	Cost of the tender (Rs. 25,000) in shape of Demand draft/ Banker's cheque.			
9.	EMD for an amount of Rs. 8,00,000 only, refundable (without interest) in shape of BG/ Demand draft/ Banker's cheque.			
10.	Bidding Forms (Section 9 – 9.1 to 9.5)			
11.	Bid Submission & Declaration form (Section 8.1)			
12.	Bidder's Authorization Certificate (Section 8.2)			
13.	Declaration of Undertaking regarding debarment and/or blacklisting (Section 8.3)			
14.	Confirmation from CSP to agree to associate (Section 7, Clause 7.2.2)			
15.	Undertaking of no conflict of Interest (Section 7, Clause 7.2.2)			

Sr. No.	Requirement	Submitted (Page No.)	Not Submitted	Remarks
16.	Contract Forms (Section 10 – 10.1 to 10.2)			

*Indicative for reference of the bidder. In case more documents are required to be submitted as per the RfP, the bidder should include the same.

Authorized Signature [In full and initials] :……

Name and Title of Signatory :……

Name of Firm: :……

Business Address :……

Bidder's Seal

Place: …….. Date: ……

13. Annexure 1 - Service Level Agreement (SLA)

13.1. Purpose of SLA

The purpose of this SLA is to clearly define the levels of service to be provided by the bidder for the duration of this contract or until this SLA has been amended. The benefits of this SLA are to:

1. SLA is between the bidder and purchaser.
2. Make explicit the performance related expectations on purchaser's requirements from the bidder
3. Assist the purchaser to control levels and performance of services provided by the bidder
4. Trigger a process that applies Purchaser and bidder management attention to aspects of performance that drop below an agreed upon threshold, or target.

13.2. Description of Services Provided

Bidder shall provide service as defined in Section 6: Scope of Work, in accordance to the definitions and conditions as defined in the Section 4: General Conditions of Contract and Section 5: Special Conditions of Contract.

13.3. Duration of SLA

This Service level agreement would be valid for entire period of contract. This SLA may be reviewed and revised as per mutual agreement.

13.4. SLA Targets

This section is agreed to by purchaser and bidder as the key bidder performance indicator for this engagement. The following section reflects the measurements to be used to track and report systems performance on a regular basis. The targets shown in the following tables are for the period of contract or its revision whichever is earlier.

SLA for Project Execution Management System (PEMS) will be decided jointly with the successful bidder before signing of contract.

13.4.1. Issue Severity Level & Resolution Time

The following section provides the service levels applicable during support period for various categories of issues.

13.4.1.1. Severity Level

Severity Level	Description	Examples
Severity 1	Environment is down, or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available	Non-availability of VM. No access to Storage, software or application

Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.	Intermittent Network connectivity
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	

13.4.1.2. IT Infrastructure SLA

S. N	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
Availability/Uptime				
1.	Availability/Uptime of cloud services Resources for Production environment (VMs, Storage, OS, VLB, Security Components,)	Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud. Measured with the help of SLA reports provided by CSP	Availability for each of the provisioned resources: >=99.5%	Default on any one or more of the provisioned resources will attract penalty as indicated below. <99.5% &>=99% (10% of the <<Periodic Payment>>) < 99% (30% of the <<Periodic Payment>>)
2.	Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / De-Activation; User Profile Management; Access Utilization Monitoring Reports) over User / Admin Portal and APIs (where applicable)	Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User / Admin Portal and APIs (where applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.5%	Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below. <99.5% and >= 99% (10% of the <<Periodic Payment>>) <99% (20% of the <<Periodic Payment>>)

3.	Availability of the network links at DC and DR (links at DC / DRC, DC-DRC link)	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud.	Availability for each of the network links: >= 99.5%	Default on any one or more of the provisioned network links will attract penalty as indicated below. <99.5% &>=99% (10% of the <<Periodic Payment>>) < 99% (30% of the <<Periodic Payment>>)
4.	Availability of Regular Reports (e.g., Audit, Certifications,) indicating the compliance to the Provisional Empanelment Requirements.	15 working days from the end of the quarter. If STQC issues a certificate based on the audit, then this SLA is not required.	5% of <<periodic Payment>>	Availability of Regular Reports (e.g., Audit, Certifications,) indicating the compliance to the Provisional Empanelment Requirements.

S. No.	**Service Level Objective**	**Measurement Methodology /**	**Target/Service Level**	**Penalty (Indicative**
Vulnerability Management				
1.	Percentage of timely vulnerability corrections	The number of vulnerability corrections performed by the cloud service provider - Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e. month, week, year, etc.). • High Severity Vulnerabilities – 30 days - Maintain 99.95% service level • Medium Severity Vulnerabilities – 90 days - Maintain 99.95% service level	99.95%	>=99% to <99.95% [10% of Periodic Payment] >=98% to <99% [20% of Periodic Payment] <98% [30% of Periodic Payment]

2.	Percentage of timely vulnerability reports	Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e. month, week, year, etc.).	99.95%	>=99% to <99.95% [10% of Periodic Payment] >=98% to <99% [20% of Periodic Payment] <98% [30% of Periodic Payment]
3.	Security breach including Data Theft/Loss/Corruption	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected INR 5 Lakhs. This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, TSECL reserves the right to terminate the contract.

S. No.	**Service Level Objective**	**Measurement Methodology /**	**Target/Service Level**	**Penalty**
RTO/RPO				
1.	Recovery Time Objective (RTO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	<= 4 hours	10% of <<Periodic Payment>> per every additional 4 (four) hours of downtime
2.	Recovery Point Objective (RPO)	Measured during the regular planned or unplanned	<= 2 hours	10% of <<Periodic Payment>> per every additional 2

		(outage) changeover from DC to DR or vice versa.		(two) hours of downtime

13.4.1.3. Resolution time

Maximum time to log the call is defined as the time taken within which help desk has to log a complaint in the system provided by the end user. Help desk should provide the trouble ticket number to the end user within 30 min of logging the complaint.

Maximum time to restore is defined as the **t**ime taken to resolve the problem, starting from the time of logging the complaint and within the time specified in table below. Help desk should notify the end user within 30 min after resolution of problem.

Severity Level	**Across all offices for the complete solution**	
	Maximum time to log the call	**Maximum time to restore**
Severity 1	30 min	240 min
Severity 2	45 min	360 min
Severity 3	60 min	480 min

13.4.1.4. Incident Management

Parameter	**Description**	**Target**	**Penalty**	**Validation tools/**
Incident logs	All incidents/ events raised with the IT helpdesk should be logged into the system by the service desk	100% calls to be logged and intimated to the end user with the trouble ticket number within the time as specified in the Notification and Resolution timetable above	1. 95%-99% calls logged: 5% penalty on the monthly Support and Maintenance charges of TSECL 2. Less than 95% calls logged and closed: 10% penalty on the monthly IT support and Maintenance charges of TSECL	1. Inspection based on count of trouble tickets for that month 2. Complaints register maintained by TSECL

Resolution of issues	All incidents/ events logged in the Incident management system should be resolved within the specified restoration time	100% of calls should be resolved within the specified resolution time specified in the table above	1. 95%-99% calls resolved: 5% penalty on the monthly IT support and Maintenance charges of TSECL 2. Less than 95% calls resolved: 10% penalty on the monthly IT support and maintenance charges of TSECL	1. Inspection based on count of trouble tickets for that month

13.4.1.5. Problem Management

Parameter	Description	Target	Penalty	Validation tools/
Root cause Identification	Vendor shall analyze all the incidents and provide a root cause report every month if there are more than 10 incidents of the same type. Vendor shall take the needed corrective action to prevent further issues due to the same cause.	100% timely submission covering all incidents logged in that month	1. 5% penalty on the monthly IT support and maintenance charges of TSECL, if the vendor does not submit a problem report for that month 2. 5% penalty on the monthly IT support and maintenance charges of TSECL, if the vendor does not perform the corrective action for more than one calendar month	1. Root cause report 2. Incident report stating problems faced by the users 3. Document detailing corrective action

13.5. Breach of SLA

In case the bidder does not meet the SLA parameters as defined above for three continuous time periods of measurement (quarters/ 3 months), the purchaser will consider this a breach of SLA and appropriate provisions under this contract will be initiated.

13.6. Exclusions

The bidder will be exempted from any non-adherence to SLAs under the following conditions:

1. Force Majeure
2. Delay due to TSECL

13.7. Warranty & Maintenance

All DC & DR hosted Infrastructure hardware / equipment supplied as part of this RFP should be provided with an in- built 3.5 years management, maintenance and software upgrade service commencing after the award of letter of award. The bidder is required to provide the prices in the relevant section of price bid. No additional amount on account of variations, omissions etc. are payable except variation in statutory taxes and duties.

Bidder shall warrant that the delivered software meets the requirements as specified in the detailed Specifications of the Application Software. This warranty shall remain valid for three (3) months after the acceptance of the software by the TSECL or three (3) months after the delivery of the software, whichever is earlier.

TSECL shall promptly notify Bidder in writing of any 'defect' in the software arising due to the reasons solely and entirely attributable to Bidder under this warranty. Upon receipt of such notification, Bidder shall remove the 'defect' in the application software.

The scope of the warranty for Project Execution Management System (PEMS) shall be limited only to correction of any bugs that were left undetected during acceptance testing by the TSECL. Warranty shall not cover any enhancements or changes in the application software, carried out after acceptance testing. This warranty is only valid for defects against approved Specifications. The above mentioned warranty shall also not apply if there is any (i) combination, operation, or use of some or all of the deliverables or any modification thereof furnished hereunder with information, software, specifications, instructions, data, or materials not approved by Bidder and operation of the deliverables on incompatible hardware not recommended by Bidder; (ii) any change, not made by Bidder, to some or all of the deliverables; or (iii) if the deliverables have been tampered with, altered or modified by the TSECL without the written permission of Bidder; or (iv) defects in components or materials provided to Bidder by TSECL in connection with the preparation of the deliverable.

In case of breach of this warranty, TSECL's exclusive remedy will be to obtain (1) the re-performance of the service or the correction or replacement of any service deliverable that provides substantially similar functionality or (2) if both parties mutually determines that such remedies are not practicable, a refund of the fees allocable to that part of the deliverable will be due to the TSECL if already paid by the TSECL.

EXCEPT AS SET FORTH IN THIS AGREEMENT, BIDDER MAKES NO WARRANTIES TO TSECL, EXPRESS OR IMPLIED, WITH RESPECT TO ANY SERVICES OR DELIVERABLES PROVIDED HEREUNDER, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ALL SUCH OTHER WARRANTIES ARE HEREBY DISCLAIMED BY THE BIDDER.

13.8. Monitoring & Auditing

Bidder will provide required reports as per the agreed date of each month or as per requirements. TSECL authority will review the performance of bidder against the SLA parameters each month, or at any frequency defined in the contract document. The review / audit report will form basis of any action relating to imposing penalty or breach of contract. Any

such review / audit can be scheduled or unscheduled. The results will be shared with the bidder as soon as possible. TSECL reserves the right to appoint a third-party auditor to validate the SLA.

Annexure 2

14. Annexure 2: Project Execution Management System (PEMS)

In recent past TSECL has leveraged various IT solutions for their business processes like billing, collection, new connection, centralized customer care center, enterprise resource planning (ERP) etc. under various Govt. of India approved major projects/ schemes like RAPDRP, IPDS, RDSS etc. TSECL is now looking to streamline the process on engaging and monitoring the physical execution of these projects so that TSECL can get the detailed information on the project execution at any certain point of time. This standalone process/ application will majorly focus on the physical progress of the projects.

At present, the three core modules of ERP i.e., Material Management (MM), Finance (FI) and Human Resource Management System (HRMS) with Employee Self Service (ESS) portal are available in existing ERP solution of TSECL.

Material Purchase, Issue, LOI Issue, Service Acceptance, Liability Creation, Vendor Payment and Asset Creation etc. are done in existing ERP system already. However, the associated physical progress documents like Inspection reports, Utilization Certificates etc. are checked and processed manually entirely on paper, which leaves a scope of human manipulation and there is no control. As a result, process compliance can be compromised. TSECL requires a system, where such a solution will be designed which will be primarily used for major and long-term projects, to maintain project specific documents at each stage, where each stage will have role-based access and corresponding approval mechanism. Once a stage is completed, then only the next stage can be accessed by user.

All relevant records will be available in the new standalone application after the projects are registered by TSECL users. Also, TSECL will be able to access and download the necessary reports based on the registered project details from this application as and when required.

The following flow chart includes high level landscape of the required **Project Execution Management System** which TSECL is looking for:

The Project Execution Management System (PEMS) will have total 5 stages as provided below:

1. **Stage-I: Contract Registration**:

   This stage is mainly for master data creation. The details of project/ scheme, contracts, BoQ, work locations, BG details etc. will be captured here.

2. **Stage-II: Material Management**:

   This stage is for capturing the whole process of movements of materials to be used in execution of the project i.e. from purchase to installation. In this stage, Inspection calls to be generated, Final Inspection approval, report upload, dispatch instruction, material received status, material acceptance and billing status etc. are to be captured here.

3. **Stage-III: Joint Measurement Certificate**:

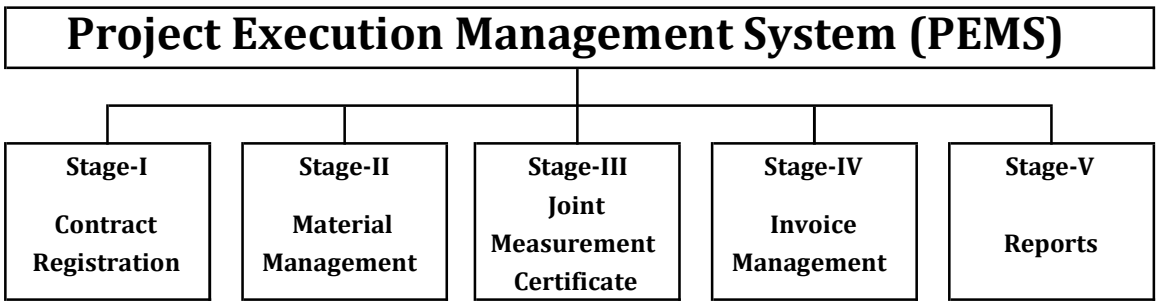
   In this stage, recording of joint measurement, details of measurement, JMC Code generation etc. are to be captured. Thereafter, uploading of SLD, signature and counter signature, approval of JMC and finally status of Hand over/ takeover to be captured.

4. **Stage-IV: Invoice Management**:

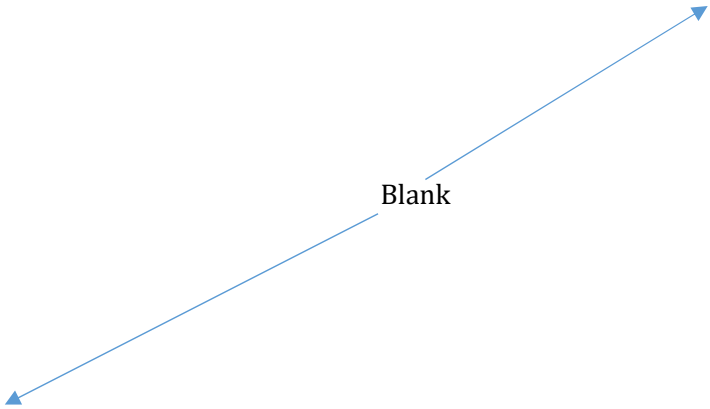
   This stage is basically to capture the details of bills and their status. Various important inputs related to bills like checklist of bills, BG, pass order, time extension details, applicable LD are to be done in this stage. Based on the input level and output level, the details are to be updated in stage-I. Some parameters are to be checked with stage-III & Stage-I and finally technical vetting to be done in this stage.

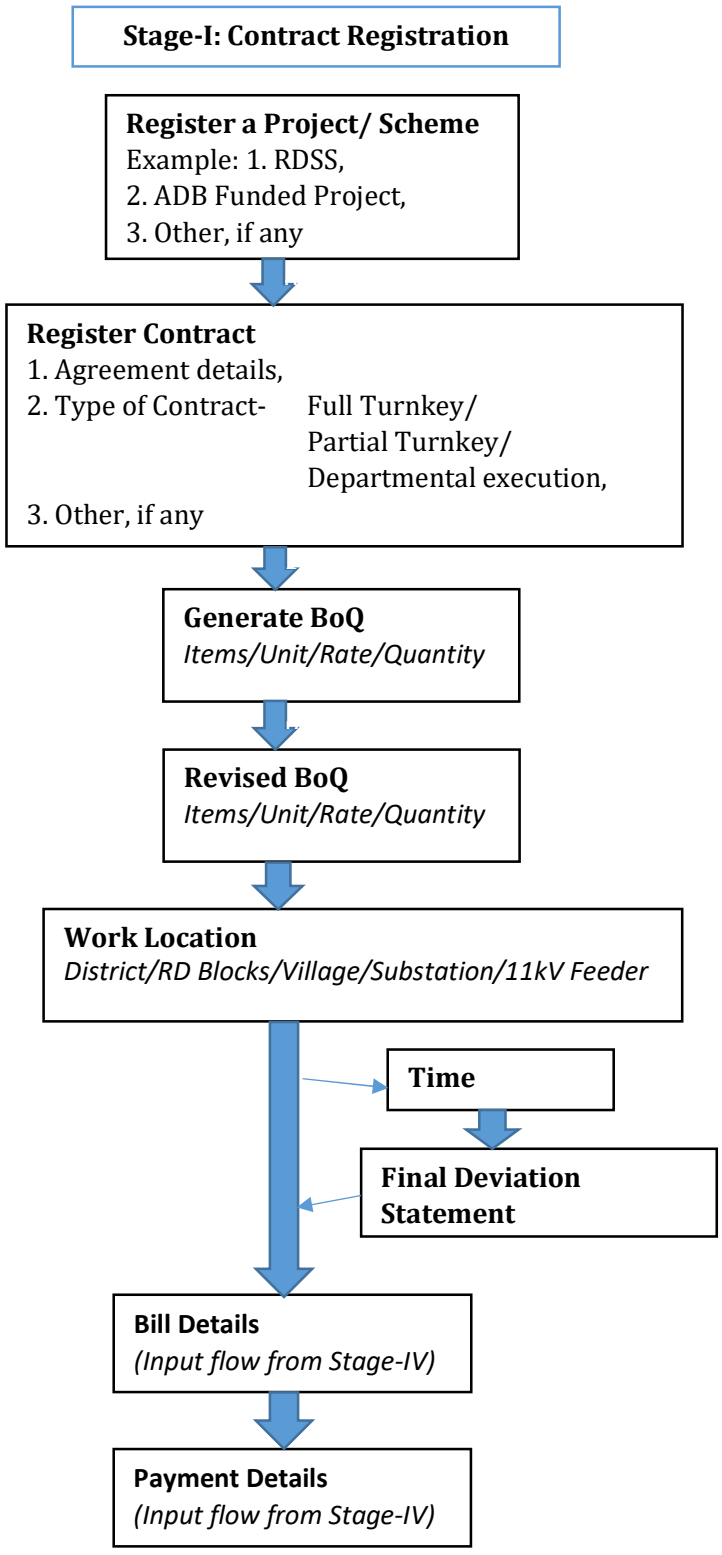
5. **Stage-V: Reports**:

   Provision for generation of various interactive reports mutually decided by the utility. Formats of these reports will be informed by the utility as and when required during the execution of the work.



A basic flow chart depicts below of the required Project Execution Management System (PEMS):




Stage-I: Contract Registration
Register a Project/ Scheme
Example: 1. RDSS,
2. ADB Funded Project,
3. Other, if any
Register Contract
1. Agreement details,
2. Type of Contract- Full Turnkey/
Partial Turnkey/
Departmental execution,
3. Other, if any
Generate BoQ
Items/Unit/Rate/Quantity
Revised BoQ
Items/Unit/Rate/Quantity
Work Location
District/RD Blocks/Village/Substation/11kV Feeder
Time
Final Deviation Statement
Bill Details
(Input flow from Stage-IV)
Payment Details
(Input flow from Stage-IV)

Stage-II: Material Management

Select Project
(Select from Drop down list)

↓

Select Contract/Agreement
(Select from Drop down list)

↓

Generate Inspection Call
Vendor Approval - Yes/No. if Yes enter Vendor

↓

Stage Inspection
Approved/Not Approved/Waived/Not Applicable

↓

Final Inspection
Approved/Not Approved/Waived
Upload Report

↓

Dispatch Instruction

↓

Material Received at Site
LR Copy - Upload/Checked/OK/Not OK
Visual Inspection –
Quality: Checked/OK/Not OK
Quantity: Checked/OK/Not OK

↓

Material Accepted

↓

Entry in Stock
1. Supplied
2. Billed (Supply)
3. Erected
4. Available in Stock

Stage-III: Joint Measurement Records

Select Project
(Select from Drop down list)

↓

Select Contract/Agreement
(Select from Drop down list)

↓

Recording of Joint Measurement (Feeder wise)

1. JMC No.- (System Generated)
2. Date of Measurement- (System Generated)
3. Measurement done by-
   1. Name/Designation/Office/Company (Utility)
   2. Name/Designation/Office/Company (PMA*)
   .
   .
   N. Name/Designation/Office/Company (TKC*)
4. Location of Work – District- (Select from dropdown list)
   RD Block (s)- (Select from dropdown list)
   Village (s)- (Select from dropdown list)
   11kV Feeder- (Select from dropdown list)
   Connecting Substation - (Select from dropdown list)
5. Details of Measurement- Item No.- (Select from dropdown list)
   Quantity-

↓

Upload SLD*
(GPS App Based/Manually

↓

Counter Signature

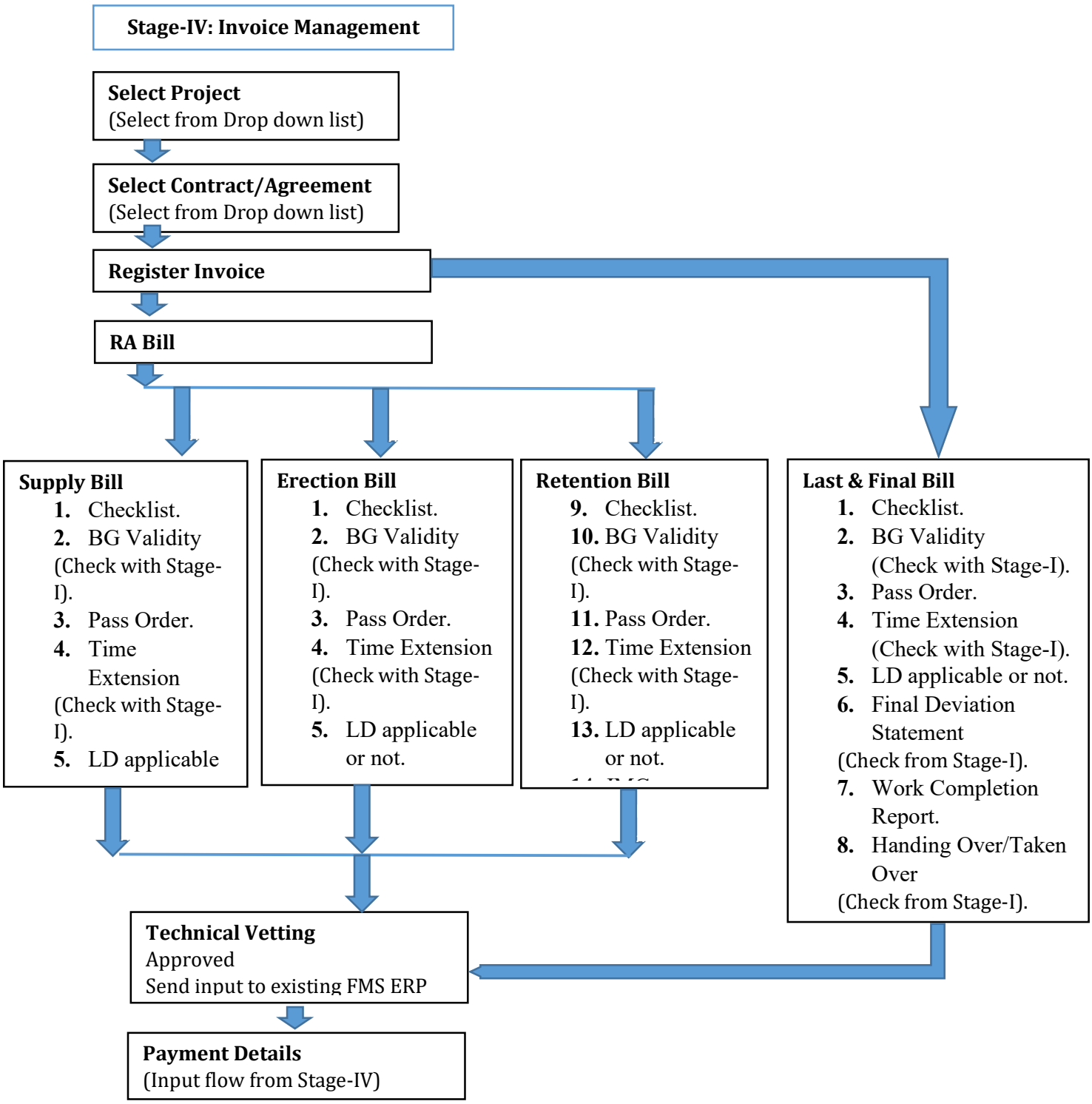
↓

Approval of JMC*

↓

Handing over/ Taken over

***Abbreviations:**
PMA - Project Management Agency
TKC - Turn Key Contractor
SLD - Single Line Diagram
JMC - Joint Measurement Certificate



*****End of document*****