ASSAM GAS COMPANY LTD.
(A GOVT.OF ASSAM UNDERTAKING)

Request for Proposal

For

Engagement of System Integrator (SI)/OEM's for procurement ICT Hardware including Installation, Configuration, Commissioning for enablement of ERP Solution at Assam Gas Company Limited (AGCL)

Tender No: AGCL/ERP/2021/02/206
Dated: 30/06/2021

Office of

Assam Gas Company Ltd.

P.O. Duliajan, District: Dibrugarh,

Assam. PIN-786602

Index

DISCLAIMER

This Request for Proposal is not an agreement. It is neither an offer nor invitation by AGCL to any Bidder other than the one that qualifies based on evaluation of submitted bids.

The purpose of this Tender Document (RFP) is to provide information to the potential Bidders to assist them in responding to this TenderDocument.

Though due care has been taken to ensure that this tender document is prepared with enough care to provide all required information to the potential Bidders. However, they may need more information than what has been provided herein.

In such cases, the potential Bidder is solely responsible to seek the information required from AGCL at its own cost. AGCL reserves the right to provide such additional information at its sole discretion. In order to respond to the Tender Document, if required, and with the prior permission of AGCL, the potential Bidder may conduct his own study and analysis as may be necessary at its own cost.

AGCL makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations on any claim the potential Bidder may make in case of failure to understand the requirement and respond to the Tender Document. AGCL may, in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this Tender Document.

ABBREVIATION

Abbreviations	Description
AGCL	Assam Gas Company Limited
CCB	Change Control Board
CMMI	Capability Maturity Model Integration
DSC	Digital Signature Certificate
DGM	Deputy General Manager
EMD	Earnest Money Deposit
FRS	Functional Requirement Specification
GST	Goods and Service Tax
ICT	Information and Communication Technology
LoI	Letter of Intent
LoA	Letter of Award
PBM	Pre-Bid Meeting
PAN	Permanent Account Number
PBG	Performance BankGuarantee
PSU	Public Sector Undertaking
PO	Purchase Order
NIT	Notice Inviting Tender
SLA	Service Level Agreement
SI	System Integrator
SRS	Software Requirement Specification
QGR	Quarterly Gross Revenue (5 Year Warranty/ O&M Phase)

1. Notice Inviting E-Tender

A. Assam Gas Company Limited (AGCL) invites E-bids from eligible System Integrators (SI) through procurement portal of the Government of Assam for the work detailed out in Table-I

B. The response to this RFP are invited from qualified, eligible and reputed OEM (Original Equipment Manufacturers)/System Integrators (SI) having sufficient technical experience and financial capabilities for successfully designing, implementing, commissioning and providing maintenance of a datacenteras detailed out in the scope of work.

Name of the Project	Period of Completion	Tender Document Cost in INR (Non-Refundable)	Earnest Money Deposit in INR (Refundable)
Request for Proposal for Engagement of System Integrator (SI)/OEM's for procurement ICT Hardware including Installation, Configuration, Commissioning for enablement of ERP Solution at Assam Gas Company Limited (AGCL)	Supply, Installation and Commissioning to be completed within 4 months from the date of LOI Warranty: all Hardware, Software & related licenses to be under warranty for 5 (Five Years) from the Date of Installation	Rs. 2,000/-	Rs. 5,00,000/-

i. The intending bidders are required to download the e-tender documents from the website http://www.assamtenders.gov.in. The non-refundable tender fee has to be remitted online.
ii. EMD to be submitted online along with the bid.
iii. The intended bidders will have to upload digitally signed Technical Bid and Financial Bid, on the website http://www.assamtenders.gov.in.
iv. The bidders must strictly adhere to the timelines as mentioned in the "Important Dates and Information" section for submission of bids.
v. This RFP will follow a 2-Part evaluation. Only those prospective bidders that qualify the technical evaluation by the AGCL Tender Evaluation Committee will be considered for opening of the Financial Bid. The decision of the 'Tender Evaluation Committee' will be final, absolute, and binding in this respect.

2. Guidelines for E-Tendering

Instructions/guidelines for electronic submission of the tenders have been provided below for assisting the bidders to successfully participate in e-Tendering.

1. **Registration of Bidder:**
   Bidders willing to take part in the process of E-Tendering will have to get themselves enrolled and registered with the Government e-Procurement System by logging on to http://www.assamtenders.gov.in.

2. **Digital Signature Certificate (DSC):**
   Each Bidder is required to obtain a Class-II or Class-III Digital Signature Certificate (DSC) for submission of tenders from the approved service provider of the National Informatics Centre (NIC) on payment of requisite amount. The bidder will use this DSC key to log on to the website through one's user ID and download NIT and BoQ. This is the only mode available for download and submission of Tender Documents.

3. **Submission of Tenders:**
   The bidders are required to submit the tenders exclusively through online mode on the government e-procurement website http://www.assamtenders.gov.in in two parts (Part-A will contain the Technical Bid and Part-B will contain Price Bid in the BoQ) before the prescribed date and time as mentioned in the "Important Dates and Information" section using the Digital Signature Certificate (DSC).

3. Important Dates and Information

1	Tender No. and Date	AGCL/ERP/2021/02/206 dated 30th June 2021
2	Tender Version	1
3	Brief description of project	Request for Proposal for Engagement of OEM/System Integrator for procurement ICT Hardware including Installation, Configuration and Implementation at Assam Gas Company Limited, Duliajan (AGCL)
4	Tender document Fee	Bidder should submit Tender Document Fee of Rs. 2000 (Two Thousand Only) online in the procurement portal of Assam Government Tenders
		Website: http://www.assamtenders.gov.in .
5	Earnest Money Deposit (EMD)	Bidder should submit Earnest Money Deposit (EMD) Fee of Rs. 5,00,000 (Five Lakh Only) online in the procurement portal of Assam GovernmentTenders http://www.assamtenders.gov.in .
6	Tender issuing entity	Assam Gas Company Limited, Duliajan (AGCL)
7	Date of uploading of N.I.T. and other Documents (Online) (Publishing Date)	Date: 30th June 2021
8	Documents download (Online)	Date: 30th June 2021
9	Last Date and time of sending the queries (Offline)	Date: 5th July 2021, 15:00 Hrs.
10	Pre-Bid Meeting (Online)	Date: 7th July 2021; 10:00 Hrs.
		• Pre-Bid meeting will be carried out on virtual platform which will intimated to the bidders later Bidders who have purchased the tender will be invited in the Pre-Bid meeting
		• Queries from SI/Bidder/OEM who do not participate in the Pre-bid meeting, will not be entertained later.
		• Queries will be sent to:
		Shri N.H Hazarika
		HOD-HSE/ERP
		AGCL, PO. Duliajan
		Dist. Dibrugarh, Assam
		E-Mail: nhhazarika@agclgas.com
11	Corrigendum, if any will be published (On-Line)	Date: 10thJuly 2021, 15:00 Hrs.; 16:00 Hrs.
12	Bid Submission start date and time (On-line)	Date: 30thJune 2021; 16:00 Hrs.
13	Bid Submission closing date and time (On-line)	Date: 15thJuly 2021; 15:00 Hrs.
14	Bid opening date and time for Technical Proposals (On-line)	Date: 15hthJuly 2021; 15:30 Hrs.
15	Date for opening of Financial Bid (On-line)	To be notified later.

16	Method of Bidder Selection	• The Project will be evaluated on L1 basis
		• The Referral bid is in Two-Part Technical and Financial Bid (Price bid)
		• The Price bids of successful Technical bidders will be opened only.
17	Contact Persons Regarding this Project	1) Shri N.H Hazarika
		HOD-HSE/ERP
		AGCL, PO. Duliajan
		Dist. Dibrugarh, Assam Pin- 786602
		E-Mail: nhhazarika@agclgas.com

4. Instructions to Bidders

4.1. Definition

In this document, the following terms shall have following respective meanings:

A. "Agreement" means the Agreement to be signed between the successful bidder and Assam Gas Company Limited (AGCL) including all attachments, appendices, all documents incorporated by reference thereto together with any subsequent modifications, the RFP, the bid offer, the acceptance and all related correspondences, clarifications, presentations.

B. "Bidder" means any firm offering the solution(s), service(s) and /or products required in the RFP. The word Bidder when used in the pre-award period shall be synonymous with Bidder, and when used after award of the Contract shall mean the successful Bidder with whom AGCL signs the agreement for supply, install, commission and render services for the systems as per the scope of the project

C. "Contract" is used synonymously with Agreement.

D. "Contract Price" means the price to be paid to the Contractor by AGCL for providing the Solution, in accordance with the payment terms defined and agreed by both parties

E. "SI/Contractor" means the Bidder whose bid to perform the Contract has been accepted by Tender Committee and is named as such in the Letter of Award.

F. "Confidential Information" means all information including AGCL Data (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, which is disclosed to or otherwise learned by the Bidder in the course of or in connection with this Agreement (including without limitation such information received during negotiations, location visits and meetings in connection with this Agreement).

G. "Deliverables" means the products, infrastructure and services agreed to be delivered by the Bidder in pursuance of the agreement as defined more elaborately in this RFP, Implementation, Operation and the Maintenance (O&M) phases.

H. "Default Notice" shall mean the written notice of Default of the Agreement issued by one Party to the other.

I. "Installation" Shall mean installation of ERP solution to achieve functional objectives defined in the RFP.

J. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a Contract 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 AGCL and eventually Govt. of Assam of the benefits of free and open competition.

K. "GoA" / "Government" / "Govt. of Assam" means the Government of Assam. "GoI" shall stand for the Government of India.

L. "Implementation Period" shall mean the period from the date of signing of the Agreement and up to the issuance of Final Acceptance Certificate for the project.

M. "Law" shall mean any Act, notification, bye law, rules and regulations, directive, ordinance, order or instruction having the force of law enacted or issued by the Central Government and/or the Government of Assam or any other Government or regulatory authority or political subdivision of government agency.

N. “LoI” means issuing of Letter of Intent shall constitute the intention of the AGCL to place the Purchase Order (P.O) with the successful bidder.

O. “Personnel” means persons hired by the Bidder as employees and assigned to the performance of the Infrastructure Solution or any part thereof.

P. “Project” means Procurement of ICT Infrastructure,its Design, Configuration, Implementation and commissioning for enablement of ERP solution and providing Warranty services for 5 years.

Q. “Project Implementation” means Project Implementation as per the testing standards and acceptance criteria prescribed by Client or its nominated agencies.

R. “Project Plan” means the document to be developed by the Contractor and approved by the Project Management Committee, based on the requirements of the Contract. The project plan may be changed/ modified during the project. Should the Project Plan conflict with the provisions of the Contract in any way, the relevant provisions of the Contract, including any amendments, shall prevail.

S. “Period of Agreement" means 5 years from the date of Go-Live of the Project.

T. “Material Breach” means a breach by either Party (Client or Bidder) of any of its obligations under this Agreement which has or is likely to have an Adverse Effect on the Project which such Party shall have failed to cure.

U. “Parties” means Client and Bidder for the purposes of this Agreement and “Party” shall be interpreted accordingly.

V. “Services” means the work to be performed by the Bidder pursuant to this Contract, as described in the detailed Scope of Work.

W. "System Integrator/ SI/ Operator" means the company providing the services under Agreement.

X. “Requirements” shall mean and include schedules, details, description, statement of technical data, performance characteristics, standards (Indian as well as International) as applicable and specified in the Contract.

Y. “AGCL” mean Assam Gas Company Limited

Z. “Termination Notice” means the written notice of termination of the Agreement issued by AGCL

AA. "Uptime" means the time period when ERP application is available with specified technical and service standards as mentioned in section titled SERVICE LEVEL AGREEMENT” "%Uptime" means ratio of 'up time' (in minutes) as mentioned in section titled “Warranty support”

BB. “Successful Implementation / Go-Live” will mean:

i. Successful deployment, commissioning and User Acceptance Testing (UAT) of the Hardware

ii. Successful Data migration after verification and approval by the Project Management Committee

iii. Achievement of the Service Levels as expected and defined during all phases

iv. Acceptance / Sign off from AGCL

v. Training and capacity building

CC. "Services" means the services delivered to the Stakeholders of Client or its nominated agencies, employees of Client or its nominated agencies, and to professionals, using the tangible and intangible assets created, procured, installed, managed and operated by the Bidder including the tools of information and communications technology and includes but is not limited to the list of services specified in this RFP.

DD. "Service Level" Means the level of service and other performance criteria which will apply to the Services delivered by the bidder.

EE. "SLA" means the Performance and Maintenance SLA executed as part of the Master Service Agreement.

FF. "Data" means all proprietary data of the Assam Gas Company Limited (AGCL) generated out of operations and transactions, documents pertaining to the ERP process.

4.2. Submission of Bid

A. The prospective bidders who have purchased the bid are required to submit their bids online on the procurement portal of Assam Government / AGCL.

B. The bids are required to be submitted/uploaded in 2 parts. Part-A will comprise of Technical Proposal and Part-B will comprise of Financial Proposal.

C. All the prospective bidders need to submit the bids in adherence with the timelines mentioned in the Important Dates and Information Section using the Digital Signature Certificate (DSC).

4.3. Query

A. The bidders will be allowed to submit their queries as a part of this RFP.

B. The last date of submission of queries is: 05th July 2021; 15:00 Hrs.

C. The queries along with the proof of purchase of tender shall be submitted in the format as provided below. Queries will be sent to the following person:

- Shri Nazrul Hussain Hazarika- (HOD-HSE/ERP)
- Email-nhhazarika@agclgas.com

D. The prospective bidders(Bidders who have purchased the tender) should send only one e-mail containing all the Pre-Bid Queries, as per format (mentioned in Table 3).

E. In case of more than one e-mail, only the queries provided in the first e-mail shall be considered.

4.4. Pre-Bid Meeting

In order to provide an avenue to prospective bidders (Bidders who have purchased the tender) for clarification of queries pertaining to this RFP, AGCL will host a virtual Pre-Bid Meeting.

A. The purpose of the Pre-bid meeting is solely to provide a forum to the prospective bidders to clarify their doubts/seek additional information pertaining to this RFP which is necessary for them to refine and submit their bid.

B. All enquiries from the bidders relating to this Bid Document must be submitted to the designated contact person as mentioned above via email. The queries should necessarily be submitted in

the followingformat (Illustrative manner of filling is provided):

#	RFP Document Reference			Content of RFP requiring Clarification	Clarification Sought
	Section Number & Name	Sub-Section Name & Clause No	Page No.		
1					
2					
3					

4.5. Cost of Bidding

The bidder shall bear all the costs associated with the bidding process including preparation and submission of bids. AGCL will not be responsible for/ liable to pay any costs regardless of the outcome of the bidding process.

4.6. Bid Document

A. It is expected on part of the bidder that he has done requisite site survey of the AGCL and examined all the instructions, forms, terms and requirement in the bid document/any additional document subsequently issued as a part of this RFP (corrigendum etc.) before submitting the bid.

B. Thus, the invitation to bid together with all its attachments thereto shall considered to be read, understood, interpreted and accepted by the bidder.

C. The bidder will not be allowed to propose any deviations post final submission of bids.

D. In an event of failure to furnish all information required by the bid document or a bid not substantially responsive to the bid document in every respect, the same may summarily be rejected.

4.7. Amendment of Bid Document

A. AGCL reserves the right at any time prior to the deadline for submission of proposals to add/modify/delete any portion of this document by issuance of a Corrigendum.

B. The corrigendum would be published on the website, will be binding on all bidders and will form part of the bid document.

C. AGCL can publish corrigendum up-to 3 days prior to the Bid submission deadline. AGCL will provide at least 7 days (through extension of bid submission deadline, as case may be) between the publishing of corrigendum and final submission deadline for bids to incorporate the modifications of Corrigendum. It is the onus of bidders to submit their bids taking into consideration all the corrigendum issued as a part of the bidding process. Any deviation requested by bidders after the Bid Submission Deadline due to non-incorporation of corrigendum will not be entertained.

4.8. Modification and Withdrawal of Bids

A. The bidder is allowed to modify/withdraw his submitted bid only before the deadline for bid submission.

B. The bidder will have to upload the entire bid documents again using DSC if he chooses to modify any component of his bid.

4.9. Language and Bid Correspondence

A. The bidder is required to prepare the proposal (including preparation of all documents that form a part of proposal which are to be supplied by the firm) in English language only.

B. The correspondence between AGCL and bidder shall be in English language and all the correspondence by mail must be subsequently confirmed by a signed formal copy.

4.10. Earnest Money Deposit

A. The bidder is required to submit an EMD (Earnest Money Deposit) as a part of this RFP. The Bidder shall pay EMD of Rs. 5,00,000 (Five Lakhs Only) online through the website: http://www.assamtenders.gov.in .

B. The detailed procedure for making payment of Tender Fees and EMD is available in the portal http://www.assamtenders.gov.in.

4.11. Forfeiture of EMD

The following actions of bidder may lead to forfeiture of EMD/PBG by AGCL:

A. Withdrawal of proposal before the expiry of the validity period

B. If it is discovered that bidder has indulged in any activity during the evaluation process that would jeopardize the bidding/ evaluation process. The decision of AGCL regarding forfeiture of EMD shall be final and shall not be called upon question under any circumstances.

C. If the bidder has violated any of the provisions of the terms and conditions of the proposal.

D. In the case of a successful Bidder, if Bidder fails to:

i. Accept the work order within the defined timelines along with the terms and conditions.

ii. Furnish performance bank guarantee (PBG) within the timelines as mentioned in this RFP.

iii. Indulges in any such activities that would jeopardize the work and violates any of the work conditions of this proposal

iv. Submit false/misleading information/ declaration/ documents/ proof/etc.

The decision of AGCL with respect to forfeiture of EMD shall be final and binding on the bidder. Besides forfeiture of EMD/BG, the bidder may also be placed on the blacklist for a period of 2 years as per the discretion of AGCL.

4.12. Forms and Formats

A. The bidder shall prepare and submit the Technical and Commercial bid as per the formats specified in this RFP. The bidder shall use the forms which are part of this RFP to provide all relevant information. The bidder may attach extra sheets in the same format if so, required by him to provide information. Where the formats /forms are not available in this RFP, the bidder shall design a form to hold the required information

4.13. Lack of Information to Bidder

A. It is expected and subsequently concluded that the bidder has carefully examined the bid document in its entirety. Any lack/misinterpretation of information is solely the responsibility of the bidder

and shall not relieve the bidder of his responsibility to fulfil his obligation under the bid. As such, any clarifications/information required by the bidder may be communicated to AGCL through E-mail before the Pre-Bid Meeting in the defined formats. The same will be clarified in the Pre-Bid meeting.

4.14. Evaluation Procedure

A. This tender is 2 stage procurement process involving Technical and Financial Evaluation of the bidder following L-1 methodology.

B. The bidders who have submitted Tender fees,Earnest Money Deposit, and NIT declaration (Part-I) as per requirement will be shortlisted for further evaluation. Absence of these documents will summarily lead to rejection of bids.

C. The Tender Evaluation Committee will evaluate the bids based on the Pre-Qualification Criteria. Those qualifying the same will be considered for further evaluation.

D. The evaluation of price bid will be based on "L-1". where the bidder with the lowest financial quote will be declared successful bidder and will be awarded the project for implementation of the solution as per Scope of Work. AGCL will/may ask all Qualified Bidders for technical presentation and understand the solution and implementation approach. AGCL TEC will have all rights reserved to disqualify any bidder basis poor understanding of the scope and non-capability of the SI to implement the solution. All participating SI/bidder must have Qualified team as asked in the Eligibility Criteria.

E. The cost quoted by the bidder shall be firm during the entire duration of the project.At the end of the contract period, the bidder will hand over (and transfer ownership of) the application software/hardware components to AGCL.

4.15. Performance Bank Guarantee

A. The bidder is required to furnish Performance Bank Guarantee (PBG) in the approved format within 21 days of notifying the acceptance of proposal for award of contract.

B. The Performance Bank Guarantee (PBG) should be from an Indian Nationalized Bank/Scheduled Bank as per Annexure-14 amounting to 10% of total bid value for the entire contract period plus 90 days beyond the contract due date as its commitment to perform services under the contract.

C. PBG which are valid for the contract period plus 90 days beyond the contract end date shall only be accepted by AGCL. In addition, bidder may be asked to extend the PBG validity according to project progress.

D. In an event of failure to comply with the requirements of the project, the event shall constitute enough and sufficient grounds for the forfeiture of the PBG.

E. AGCL shall release PBG after expiry of contract/post completion of work according to contract conditions provided there is no breach of contract on part of bidder. AGCL will not pay any interest on the PBG.

4.16. Awarding of Contract

A. The project will be awarded to the successful bidder post an affirmative Post Qualification determination.

B. A negative determination will lead to the rejection of the bidder's bid. In such an event, AGCL reserves the right to proceed to next evaluated bidder to carry out a similar assessment of that bidder's capacity to execute the project satisfactorily

C. The contract will be awarded by AGCL to the successful bidder whose bid has been determined to be substantially responsive after the completion of final negotiations, if required.

D. The successful bidder(s) will have to furnish a Performance Bank Guarantee (PBG) as per Annexure-14, amounting to the 10% of the total bid value for the entire contract period plus 90 days within 21 days for acceptance of proposal for award of contract, as its commitment to perform services under the contract

4.17. Contract Execution

A. The contractor is required to submit a Performance Bank Guarantee (PBG) within 21 days from the receipt of Letter of Award. The validity of PBG should be contract period plus 90 days beyond the contract end date. The validity of PBG may be extended at the discretion of AGCL.

4.18. Liquidated Damages

If the Bidder fails to complete the work within the agreed time schedule (Project Time Line) as specified in the Contract Agreement or any extension thereof, AGCL shall recover Liquidated Damage from submitted invoices from the Bidder as per calculation detailed in the table mentioned below. Equipment / work will be deemed to have been delivered / completed, only when it's all components, Parts / all item of works are also delivered / completed. If certain components / items of equipment / work are not delivered in time, the same will be considered as delayed until such time due missing / incomplete parts / item of works are delivered / completed.

S No	Milestone	Severity	Liquidated Damage	Remarks
1	T0+4 Weeks Months = M1	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If fail incompletion of works and delivery for more than 5 week, letter of Default will be issued for Improvement.
2	T0 + 10 Weeks Months = M3	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value ofthe affected deliverables	Iffailindeliveryfor more than 5 week, letterofDefaultwill be issuefor Improvement.
3	T0+ 16 Weeks (T1) Months = M4	Critical	0.5% per week of the affected deliverables subject to a maximum of 10% of the value ofthe affected deliverables	If delay is more than 5 weeks then, payment of equipmentdelivery will be hold.

S No	Milestone	Severity	Liquidated Damage	Remarks
4	T0+20 Weeks Months =M5	Critical	1.0 % per week of the affected deliverables subject to a maximum of 10% of the value ofthe affected deliverables	If delay is more than 5 weeks then, payment of equipmentdelivery will be hold.
5	T0+32 or T1+16 Weeks Months =M8 (Project Sign-Off & FAT (Go-Live of the Project by ERP Solution Provider)	Critical	1.0 % per week of the affected deliverables subject to a maximum of 10% of the value of the affected deliverables	If delay is more than 5 weeks then, payment of equipment delivery will behold. If delay is more than 10 weeks then, AGCL is free to cancel the WO/contract. The remaining partof work will be completed by any agency engaged by AGCL

"T0" is the Project Initiation Date

4.19. Annual Technical Support

The vendor has to provide annual technical support post end of Go-Livefor a period of 5 years.As a part of Support, SI will provide support in the form of installation of all necessary patches/updates as and when released by OEM and incorporate any changes suggested by AGCL or required as per change in statutory laws and regulations and also attend to breakdown if any.

4.20. Penalty

AGCL reserves the right to impose a suitable penalty as mentioned under the (Liquidated Damages and Penalties) section of this RFP in case of any delay/ non-performance from their end.

4.21. Suspension of Work

A. AGCL shall have the right to suspend the progress of the work, or any of its part through a notice to the contractor and due to any reason, it deems adequate for such an action. Contractor will be obligated to suspend the further progress of the work until further communication/notice is received from AGCL.

B. The contractor shall also be obligated to recommence work immediately after receiving a notice in writing from AGCL.

C. The AGCL shall have the exclusive right/discretion to compensate/not to compensate whole or any part of the time lost for such delay or suspension

4.22. Liability

A. In an event where the bidder is at fault, AGCL shall be entitled to recover damages from the contractor.

B. In each such instance, regardless of the basis on which AGCL is entitled to claim damages from the Contractor (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), the liability of the contractor will be limited to the total net value of the project.

C. Liability for any damage to real and tangible property or bodily injury (including death) limited to that cause by the Contractor's negligence.

D. As to any other actual damage arising in any situation involving non-performance by Contractor pursuant to or in any way related to the subject of this Agreement, the charge paid by AGCL for the individual product or Service that is the subject of the Claim.

E. However, the contractor shall not be liable for:

   a. Any indirect, consequential loss or damage, lost profits, third party loss or damage to property or loss of or damage to data and reputation.

   b. Any direct loss or damage that exceeds the total value for Contract Price made or expected to be made to the Contractor hereunder.

4.23. Governing Laws

A. This contract is governed by the laws in force in India. The courts at Dibrugarh shall have exclusive jurisdiction in all matters arising under the contract.

B. It is solely the responsibility of the Contractor to keep himself fully informed of all current national, state and municipal law and ordinances and take due care that such are not infringed upon by the actions of the contractor. The Contractor shall obtain all necessary permits and licensed and pay all fees and taxes required by law at their own expense. These will be entirely contractor's obligation to protect itself from any claim of infringement and in no way AGCL will be liable for any such losses to the contractor

4.24. Termination for Default

A. AGCL reserves the right to terminate this order, either in whole or in part without prejudice to any other remedy or right of claim for breach of contract, by giving a written notice of default of at least 30 days.

B. AGCL also reserves the right to terminate the contract if the contractor fails materially, to render any or all the services within the time period specified in the contract or any extension thereof granted by AGCL in writing and fails to remedy its failure within a period of thirty days after receipt of default.

4.25. Bankruptcy

A. AGCL shall be at a liberty to terminate the contract without any notice in writing to contractor/liquidator, if the contractor becomes bankrupt/insolvent or has proceedings initiated against it by its creditors in NCLT under IBC or any other laws. Upon such termination, AGCL will not be liable to pay any compensation or obligated to provide such liquidator or receiver or other person, the option of carrying out the engagement subject to their providing a guarantee for the due and faithful performance of the engagement.

4.26. Force Majeure

A. In the event of either party being rendered unable by `Force Majeure' to perform any obligation required to be performed by them under the contract, the relative obligation of the party affected by such `Force Majeure' will stand suspended for the period during which such cause lasts. The word `Force Majeure' as employed herein shall mean Acts of God, flood, earthquake, pandemic lightening, unexpected reservoir behavior, war, fire, revolt, agitation, riot, blockade, Act of terrorism, embargo of goods/ or embargo on people, sabotage, civil commotion, road barricade (but not due to interference of employment problem of the Contractor), acts of government of the two parties, which makes performance impossible or impracticable and any other cause, strike or lockout either parties operation in that region. Direct or indirect consequences of war (declared/undeclared), sabotage, National Emergency or any Law or Promulgation, Regulation or Ordinance whether Central or State or Municipal, Breakage, Bursting or Freezing of Pipeline, whether of kind herein enumerated or otherwise which are not within the control of the party to the contract and which renders performance of the contract by the said party impossible.

B. Upon occurrence of such cause and upon its termination, the party alleging that it has been rendered unable as aforesaid thereby, shall notify the other party in writing within Seventy Two (72) hours of the alleged beginning and ending thereof, giving full particulars and satisfactory evidence in support of its claim.

C. Provided that in case such force majeure lasts for more than two (2) months the either party hereto shall be free to terminate the contract by a written notice of Fifteen (15) Days to the other party.

D. During the period for which Force majeure condition lasts, AGCL Shall make all payments basis the Work completed as per the scope of the PO and all payments for the material delivered as per the PO

E. The SI/Bidder shall not be responsible for any failure to perform, due to unforeseen circumstances

or to causes beyond their reasonable control, including but not limited to Acts of God, pandemic, war, riot, embargoes, acts of civil or military authorities, humidity, exposure to moisture, fire, floods, accidents, terrorist activities, disputes, strikes or shortages of transportation, facilities. In the event of any such aspect being beyond the control of participating agencies, appropriate strategies would be worked out as per the terms mentioned above to compensate the project activities/schedules accordingly.

4.27. Insurance Coverage

A. The contractor at their own cost shall arrange, secure and maintain all relevant insurance to cover their personnel. The Contractor responsibility towards material remain till the material is delivered at AGCL Store / offices / site where AGCL recommends delivering the material.

B. It is the responsibility of the contractor alone to maintain adequate insurance coverage at all-times. The Bidder's failure in this regard shall not relieve them of any of his contractual responsibilities, obligations and liabilities.

C. All insurance taken out by Contractor or their sub-contractor shall be endorsed to provide that the underwriters waive their rights of recourse on the Company and to the extent of the liabilities assumed by Contractor under this Contract.

4.28. Corrupt and Fraudulent Practices

A. The tender evaluation committee have the right to reject a proposal for award, if it finds that the bidder has engaged in any corrupt or fraudulent practices in competing for the contract in question.

B. The tender evaluation committee may also blacklist such firms who have engaged in fraudulent/corrupt practices for a period of 2 years from the date of detection of such acts.

4.29. Binding Clause

A. The decisions taken by Tender Evaluation Committee pertaining to the evaluation of this tender and subsequent award of contract shall be final and binding on all parties concerned. The Tender Evaluation Committee reserves the right:

   a. To vary, modify, revise, amend or change any of the terms and conditions mentioned above and,

   b. To accept or reject any or all bids 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 of the grounds for Company's action.

4.30. Warranty

The Bidder is required to provide warranty valid for Five (5) Years, for all supplied equipment as per financial bid format provided in the RFP. All Products supplied under the RFP should not reach end of support before 7 years from the date of start of Warranty Services. All the ICT infrastructure products quoted should be supported by the SI for next 5 years from the start date of Warranty.

A. The Bidder shall warrant that all the equipment supplied under the contract is newly manufactured and shall have no defect arising out of design, materials or workmanship or from any act or omission of the Bidder that may develop under normal use of the supplied equipment's in the conditions prevailing across the country.

B. The Bidder shall warrant that the services provided under the contract shall be as per the Service Level Agreement (SLA) defined in the RFP.

C. This warranty, for all equipment's, shall remain valid for Five (5) Years after the Go –Live/ Final Acceptance of Solution of the Data Centre whichever is later. The installation will be deemed incomplete if any component of the equipment or any documentation/media is not delivered or is delivered and not installed and/or not operational or not acceptable to AGCL after final acceptance testing.

D. AGCL shall promptly notify the Bidder about any claims arising under this warranty. Upon receipt of such notice, the bidder shall repair/ replace/ reconfigure/ re-provision the defective equipment or service.

E. During warranty period, maintenance of all stores including pick-up of the faulty equipment for repair, replacement and repair/fault rectification, delivery ofthe rectified equipment shall be undertaken by the supplier at no additional cost to the buyer. The supplier will be responsible for the maintenance/preventive maintenance of the complete system. Any Malfunctioning or defective items shall be replaced by the supplier free of cost at project site as early as possible, under the following condition:-

F. If the bidder, having been notified, fails to remedy the defect(s) within the period specified in the SLA, AGCL may proceed to take such remedial action as may be necessary at the Bidder's risk and expense and without prejudice to any other rights, which AGCL may have against the Bidder under the contract.

G. All the software's used for providing data Centre services shall be licensed to AGCL and will be the property of AGCL.

H. The SI shall be responsible for end-to-end implementation and shall quote and provide/supply any items not included in the bill of material but required for commissioning of datacenter. AGCL shall not pay for any such items, which have not been quoted by the SI in the bid but are required for successful completion of the project.

I. As part of the Warranty services, the bidder (system integrator) shall provide warranty support post installation and commissioning on the installed ICT infrastructure

J. The system integrator (SI) shall appoint a single-point-of-contact (SPOC) for coordination of warranty support activities including but not limited to problem tracking, problem source identification, problem impact (severity) determination, bypass and recovery support, problem resolution, and management reporting.

K. Post warranty, all components will be handed over to the AGCL in working condition (both individual and integrated ones), failure of which will be considered as a non-conformance and will attract relevant penalties under this contract.

L. The support will be onsite during AGCL business hours (8:00 A.M to 4:00 PM Monday to Friday and 8:00 AM to 12:00 noon Saturday), with access to SI to provide a maximum turnaround time of 4 hours.

M. There should not be any limits on the number of incidents reported to the manufacturer. AGCL shall have access to the online support and tools provided by the OEM manufacturer. AGCL shall also have 24x7 accesses to a variety of technical resources (personnel) as per the SLA over call/ mail including the manufacturer's knowledge base with complete collections of technical articles and system operating manuals.

4.31. Enforcement of Terms

A. Either party's failure to enforce at any point of time, the provisions of this contract or any rights in respect thereto or to exercise any option here in provided shall in no way be construed to be a waiver to such provisions, rights or options or in any way to affect the validity of the contract.

B. The exercise by either party of any of its rights herein shall not preclude or prejudice either party from exercising the same or any other right it may have hereunder.

4.32. Period of Validity of Offer

A. Bids shall remain valid for 180 days from the date of closing of bid prescribed by the Company. Bids of shorter validity will be rejected as being non-responsive. If nothing is mentioned by the bidder in their bid about the bid validity, it will be presumed that the bid is valid for 180 days from Bid Closing Date. During the period of validity of proposals, the rates quoted shall not change.

4.33. Taxes and Duties

A. The prices are to be quoted as per BoQ available separately as a part of this RFP.

B. AGCL shall deduct all statutory and necessary Tax from each bill as per Government Order prevailing at the time of payment. In addition, AGCL shall provide necessary tax deduction certificate on demand by the SI.

C. Bidder submitting a tender shall submit up to date Income Tax and Profession Taxes Certificate as well as the GST certificate issued by the concerned Tax Authority or a Certificate that the assessment is under consideration. All such clearance certificates shall be valid on the last date of permission.

4.34. Discrepancies in the Bid

A. Discrepancy between description in words and figures, the rate which corresponds to the words quoted by the bidder shall be taken as correct and final.

B. Discrepancy in the amount quoted by the contractor due to calculation mistake of the unit rate and quantity, the unit rate shall be regarded as firm and amount corrected.

4.35. Bid Due Date

A. The bid to be submitted by the bidder complete in all respects not later than the Bid Submission due date as specified in the "Important dates and Information" section and any subsequent corrigendum/ extension thereof. AGCL may at its discretion, on giving reasonable notice online, extend the bid due date. In such case, all rights and obligations of the AGCL and the bidders, previously subject to the bid due date, shall thereafter be subject to the new bid due date as extended.

B. All bids must be submitted online. Any offline bid submitted to AGCL will not be accepted / considered until and unless communicated by AGCL

4.36. Late Bid

A. Late bid will not to be accepted by AGCL. Any bids/ documents received after the bid submission date as mentioned the Important dates and Information section will not be evaluated and summarily rejected.

4.37. Opening of Bid by AGCL

A. The bidders shall be invited to attend the bid opening virtually and they may attend if they so choose. AGCL at its discretion, during bid opening may announce the bidders name, withdrawals, and the presence or absence of relevant Bid Security and such other details.

4.38. Contacting AGCL

A. The bidders should approach the AGCL officers only within the working hours (Monday to Friday- 8:00 A.M to 4:00 PM and Saturday 8:00 AM to 12:00 Noon), if necessary, before submission of the bid. No bidders shall be entertained during evaluation process.

B. Any effort made by bidder to exert any undue influence on AGCL officials in the decision on Bid evaluation, bid comparison or finalization may result in rejection of the Bidder's offer and subsequent blacklisting of the bidder for a period of 2 years. If the bidder wishes to bring additional information to the notice of AGCL, it should be in writing.

4.39. AGCL's Right ToReject Any or All Bids

AGCL reserves the right to reject any/all bids and cancel the tender without assigning any reason whatsoever.

4.40. Bid Currencies

Prices shall be quoted in Indian Rupees only, exclusive of all prevailing taxes, levies, dutiesetc.

4.41. Price

A. Price should be quoted in the BoQ only and uploaded under Price bid section in e-tender portal.

B. Price quoted should be firm, exclusive of all charges, taxes and duties.

4.42. Formats and Signing of Bid

A. All the requisite documents which are part of this RFP, including proposals, forms, RFP document issued by AGCL shall be digitally signed by an authorized signatory on behalf of the Bidder using Digital Signature.

B. The authorization shall be provided by written Power of Attorney (POA) on the Non-Judicial stamp paper of a value of INR 100 accompanying the proposal.

C. All pages of the proposal shall be initialed by the authorized person or persons signing the proposal.

D. The proposal shall contain no interlineations, erase or overwriting. Withdrawal of Bid

E. The bidders can withdraw/ modify their bids only before the Bid Submission due date. Withdrawal of bids is not allowed by the bidder during the interval between their submission and expiry of Bid's validity period.

4.43. Interpretation of Documents

A. In an event where the bidder finds discrepancies or omission in the specifications or other tender documents,or if he is in doubt as to the true meaning/interpretation of any part thereof, the bidder has right to make a written request to the tender inviting authority for correction/clarification or interpretation at the time of submission of Pre-Bid query or can put in a separate sheet along with his technical bid document.

B. However, AGCL reserves the right not to amend/provide any clarification to the queries received after submission of bids.

4.44. Preparation of Tender

Tender shall be submitted in accordance with the following instructions:

A. Tender shall be submitted in the prescribed forms. Where there is conflict between the words and the figures, the words shall govern.

B. Tenders shall not contain any recapitulation of the work to be done. Alternative proposals will not be considered unless called for. No written, oral, telegraphic or telephonic proposals for modifications will be acceptable.

C. Tenders subject to any conditions or stipulations imposed by the bidder are liable to be rejected.

4.45. Compliance with Law

A. The contractor agrees that it shall comply with all the laws including local, state and union, regulations and ordinances during discharge of his duties including procurement of licenses, permits certificates and payment of taxes under this contract.

B. It shall be the responsibility of the contractor to establish and maintain all proper records required by any law, code/practice of corporate policy applicable to it from time to time including records and returns as applicable under labourlaw.

4.46. Clarification of Bids

A. During evaluation of the bids, the Customer/Tender Committee, at its discretion may ask the bidder to provide clarification of its bid. The request for the clarification and the response by the bidder to same shall be in writing (physical letter/email) and no change in the substance of the bid shall seek offered or permitted. The bidders are required to respond to such queries/clarifications if any, within the stipulated timelines in the query document failing which their bid will liable to be rejected.

4.47. Quality Control

A. The AGCL, bidder/contractor and third party PMO shall work closely during execution of this project. The contractor as such, should act within its authority and abide by any directive issued by AGCL/Third Party PMO on implementation activities.

B. It is the responsibility of the contractor to abide by the safety measures and AGCL will not liable for any compensation/ responsibilities arising from accident/loss of life, the cause of which is due to their negligence.

C. The contractor will treat all the data and information collected about the system, obtained during execution of this project as confidential and shall not divulge such information to any third party without prior written permission of AGCL.

D. AGCL reserves the right to inspect all phases of contractor's operation to ensure conformity to the specifications as per this contract. The contractor shall allow AGCL or its designated representatives (including Third Party PMO) free access to the work at all times.

E. All disputes are subject to Court of Dibrugarh jurisdiction.

4.48. Authentication of Bids

A. The Proposal should be accompanied by a valid power-of-attorney executed on a Non-Judicial Stamp paper of value not less than INR 100 in the name of the signatory of the Proposal.

4.49. General Terms

A. The bidder is required to submit all the bid documents digitally signed by the authorized signatory, failing which the bid is liable to be rejected

B. All pages of Bid submitted by the bidder should have serial number with proper indexing.

C. All the documents to be submitted by the bidder along with their offer should be duly authenticated by the person signing the offer and if at any point of time during procurement process or subsequently it is detected that documents submitted are forged/tampered/manipulated in any way, the total responsibility lies with the bidder and AGCL reserves the full right to take action as may be deemed fit including rejection of the offer and such case is to be kept recorded for any future dealing with them.

D. The proposal should be accompanied with a forwarding letter in the letter head of the bidder duly signed stamped by the authorized signatory containing the details of the enclosures

E. All the queries either technical or commercial should be clarified at the time of Pre-Bid meeting. AGCL may not entertain any queries after opening of bids.

F. In case of discrepancy in the amount quoted by the bidder due to calculation mistake, the unit rate shall be regarded as firm and the totals shall be calculated accordingly.

G. The bids must be accompanied with a letter of complying to the Pre-Qualification criteria. otherwise the bid of the bidder will not be accepted.

H. The price offers shall remain firm within the currency of contract and no escalation of price will be allowed.

I. The bidder will automatically be informed at the time of opening of the price bid from e-tender portal.

J. No variation in or modification of the terms of the Agreement shall be made except by written amendment signed by the parties.

4.50. Exit Management

A. The SI shall not exit from the contract within stipulated time period of five (5) years after Go-Live. However, in the event that the SI decides to opt out of the contract prematurely it has to notify the authority six months in advance through a written letter, SI will not seek ownership rights over the equipment and its PBG will also be forfeited.

B. If the SI exits from the contract during the execution within the stipulated time period then AGCL reserves the right to terminate the contract and may ask the bidder with L2 price to match the price of L1 and execute the remaining work as per RFP scope of work.

C. The SI shall document and submit a detailed Exit Management Plan (EMP) at AGCL for approval within 30 days post signing of the contract. The Exit Management Plan shall be re- drafted/ reviewed by SI in annual basis and need to be submitted to AGCL.

4.50.1. Purpose of Exit Management Plan

A. This clause sets out the provisions which will apply upon completion of the contract period or upon termination of the agreement for default of the System Integrator. The Parties shall ensure that their respective associated entities, in case of AGCL, any PMO/Agency appointed by AGCL and in case of the System Integrator, the sub- contractors, carry out their respective obligations set out in this Exit Management Clause. Exit Management criteria will be a part of Master Service Agreement with detailed information about exit criteria and exit management plan.

B. The exit management period starts, exactly period of 30 days before, in case of expiry of contract, or on the date when the contract comes to an end and up to period of 30 days in case of termination of contract, or on the date when the notice of termination is sent to the System Integrator. The exit management period ends on the date agreed upon by AGCL or one year after the beginning of the exit management period, whichever is earlier.

C. The System Integrator shall divest all the project assets at the beginning of the Exit management period to AGCL at zero value in case of expiry of contract and at the depreciated rate as per Indian Income Tax Act if there is a termination of contract.

D. The System Integrator shall pay all transfer costs and stamp duty applicable on transfer of project assets.

E. At the beginning of the exit management period, the System Integrator shall ensure that:

   i. All Project Assets including the hardware, software, documentation and any other infrastructure shall have been cured of all defects and deficiencies as necessary so that the Project is compliant with the Specifications and Standards set forth in the RFP, Agreement and any other amendments made during the contract period;

   ii. The System Integrator delivers relevant records and reports pertaining to the Project and its design, engineering, operation, and maintenance including all operation and maintenance records and manuals pertaining thereto and complete as on the Divestment Date

   iii. On request by AGCL, or any PMO/Agency appointed by AGCL, the System Integrator shall effect such assignments, transfers, licenses and sub-licenses related to any equipment lease, maintenance or service provision agreement between System Integrator and any PMO/Agency, in favor of AGCL, or any PMO/Agency appointed by AGCL, if it is required by AGCL.

   iv. The System Integrator complies with all other requirements as may be prescribed under Applicable Laws to complete the divestment and assignment of all the rights, title and interest of the System Integrator in the Project free from all encumbrances absolutely and free of any charge or tax to AGCL or its nominee.

4.50.2. During Exit Management Period

A. The System Integrator will allow AGCL, or any third party appointed by AGCL access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable AGCL or any PMO/Agency appointed by AGCL, to assess the existing services being delivered;

B. Promptly on reasonable request by AGCL or any PMO/Agency appointed by AGCL, the System Integrator shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with the "Contract", the Project Plan, SLA and scope of work, relating to any material aspect of the services. Such information shall include details pertaining to the services rendered and other performance data. The System Integrator shall permit AGCL or any PMO/Agency appointed to have reasonable access to its employees and facilities as

reasonably required by AGCL, or any PMO/Agency appointed to understand the methods of delivery of the services employed by the System Integrator and to assist appropriate knowledge transfer.

C. Before the end of exit management period, the System Integrator will assist in a successful trial run of Network administration, Facility management including helpdesk management by AGCL, or any PMO/Agency appointed.

4.50.3. Handover of Assets/Documents

SI shall handover the peaceful possession of Project Assets in good and working condition with detail list showing the name of the equipment and with configuration to the Purchaser/replacement SI as authorized by Purchaser customer within 30 days of the date of serving of notice or within the Transition Period.

The SI shall provide all such information available with it during the contract execution or during the Operation & management phase as may reasonably be necessary within a reasonable period not exceeding 30 days of the date of serving of notice or within the Transition Period.

Existing SI will hand over the documents to AGCL or new SI, pertaining to the operation of Datacenter i.e. all configuration records, purchase orders, installation reports, FAT/PAT records, SLA records, SLA methodology, SLA calculation template, MIS reports, ISO documents (procedures, records, templates, standards), Audit records, security assessment and risk records, all SOPs, warranty documents, AMC documents, Knowledge documents (KEDB), Training records etc

4.50.4. Transfer of Certain Agreements

A. On request by AGCL the Bidder shall affect such assignments, transfers, licenses and sub- licenses as AGCL may require and which are related to the services and reasonably necessary for the carrying out of replacement services by the AGCL or its nominated agency or its Replacement Bidder. All Licenses and Devices have to be registered in name M/s. AGCL and name of officer from AGCL will be shared at time of signing of agreement.

4.51. Change of Scope

AGCL may, notwithstanding anything to the contrary contained in this Agreement, require the System Integrator (SI) to make modifications/alterations to the Works ("Change of Scope") before the issue of the Completion Certificate.

This can be done by AGCL, either by giving an instruction or by requesting the System Integrator to submit a proposal for Change of Scope involving additional cost or reduction in cost. Any such change in scope shall be made and valued in accordance with the provisions contained herein.

A. Change of Scope shall mean:

   i. Any Change in the specifications of any item defined in the Scope of Works including omission of any work from the scope of the project.

   ii. Any additional work that is to be carried out including procurement of software, hardware, materials or services which are not included in the defined Scope of the Project, which is the part of this RFP, including any associated Tests on completion of implementation.

B. It shall be the obligation of the System Integrator to determine and prepare a proposal with relevant details at its own costs if it establishes that a change of scope will achieve the following, if adopted:

   i. Accelerate completion

   ii. Reduce the cost to the authority of implementing, operating and maintaining the Project

iii. Improve efficiency or value to the authority of completed project

iv. Be of benefit to AGCL

C. The System Integrator shall submit such proposal. The proposal shall be supported by relevant documents and shall contain the reduction/escalation in the Contract Price if any. AGCL shall within 15 days of receipt of proposal from System Integrator either accept (as is or with modifications, if any) or reject the suggested change in Scope of Work. The System Integrator shall not undertake any change/deviation in Scope of Work without written intimation from AGCL. AGCL in written discussion along with SI and AGCL may request to change the scope. In case there is commercial implication SI will give the estimation of the same and SI may execute the same after receiving written confirmation from AGCL.

4.51.1. Procedure for Change of Scope

A. In any event where AGCL determines that a Change of Scope is necessary, it shall issue a written notice to System Integrator specifying in detail the works and services modified/added/deleted under the Change of Scope notice. The System Integrator on receipt of Change of Scope notice shall provide AGCL the following information/documentation as necessary: Impact of Change of Scope on the project completion schedule. if the works and the services are required to be carried out as per originally agreed upon timelines.

B. A detailed plan containing the options for implementing the proposed Change of Scope and the cost implication of each option including the following details:

i. break down of the quantities, unit rates and cost for different items of work.

ii. proposed design and report for the Change of Scope; and

iii. proposed modifications, if any, to the Project Completion Schedule of the Project.

Both AGCL and System Integrator agrees that, the contract price may increase/reduce on account of Change of Scope.

C. The System Integrator's quotation of costs for the Change of Scope shall be determined on the basis of prevailing market rates as determined by AGCL.

D. Upon reaching an agreement, AGCL shall issue a Change of Scope Order requiring the System Integrator to proceed in accordance with the modified Scope of Work. In the event that the Parties are unable to agree, the Authority may:

i. Issue a Change of Scope Order requiring the System Integrator to proceed with the performance thereof at the rates and conditions approved by AGCL, till the matter is resolved in accordance with Dispute resolution process; or

ii. Proceed in accordance with Power of Authority to undertake works

4.51.2. Payment for Change of Scope

A. Payment for Change of Scope shall be made in accordance with the payment schedule specified in the Change of Scope Order.

4.51.3. Restrictions on Change of Scope

A. System Integrator shall not undertake any change in scope until the issuance of Change of Scope order by AGCL.

B. The total value of all Change of Scope orders shall not exceed 10% of the contract Price unless mutually agreed by the parties.

C. Notwithstanding anything to the contrary in this section no change made necessary because of any default of the System Integrator in the performance of its obligations under this Agreement shall be deemed to be Change of Scope, and shall not result in any adjustment of the Contract Price or the Project Completion Schedule.

4.51.4. Power of the Authority to Undertake Works

A. In the event the Parties are unable to agree to the proposed Change of Scope Orders, the Authority may, after giving notice to the System Integrator and considering its reply thereto, award such works or services to any person / company on the basis of open competitive bidding from amongst bidders who are pre-qualified for undertaking the additional work.

B. The System Integrator in such an instance shall have the option of matching the first ranked bid in terms of the selection criteria, subject to payment of 2% (two per cent) of the bid amount to the AGCL and thereupon securing the award of such works or services.

C. For exercising the above option, it is mandatory for the System Integrator to participate in the bidding process and for the bid to be not more than 5% of the L1 bid.

D. The works undertaken in accordance with this section shall conform to the Specifications and Standards of RFP and Change of Scope order thereof and shall be carried out in a manner that minimizes the disruption in operation of the Project.

5. Introduction and Objective of the Project

5.1. Overview of Assam Gas Company Limited

A. Assam Gas Company Ltd., a Govt. of Assam Undertaking was incorporated on March 31st, 1962 in Shillong as a limited company wholly owned by the Government of Assam to carry out all kinds of business related to natural gas in India.

B. Assam Gas Company Limited (AGCL), has a network of underground natural gas transmission and distribution pipelines and presently serves about 400 industrial consumers (mainly tea factories), 1000 commercial establishments, more than 35,000 domestic consumers and several bulk consumers in the districts of Dibrugarh, Tinsukia, Sibsagar, Charaideo, Jorhat and Golaghat in Assam. The company owns and operates over 750 kms of steel gas pipelines and about 2500 kms of PE distribution pipelines. The company is headquartered at Duliajan in Dibrugarh district, Assam having a capacity to transport more than 6.5 MMSCM of natural gas per day. Presently Piped Natural gas is supplied to domestic and commercial consumers in 12 (Twelve) towns of Assam. There are about 20 (twenty) supply points feeding gas from E&P companies, namely OIL and ONGCL.

C. In each of the towns where the company has operations, there is a site office with limited number of employees and a Coordination Office at Guwahati. The company has about 406 employees on its rolls of which 81 are executives distributed over 7 (seven) grades and 360 are staffers and supervisors distributed over 10 grades. In addition to the permanent employees, the company has about 20 contractual employees and engages about 100 home guards stationed at various locations. VDP (village defense parties) are also engaged to secure vulnerable locations.

D. The company is a leading Govt of Assam undertaking which has been consistently making profits and paying dividend to the Govt of Assam. Turnover for 2019-2020 was Rs 368.63 Crores with PAT of Rs 82.55 Crores.

E. The company has reserves of around Rs 805 Crores which may be deployed in various projects.

F. The Chief Executive of the company is the Managing Director who is the lone full time Director on the Board. All members of the Board of Directors are appointed by the Govt of Assam except a nominee director of Oil India Ltd. The company operates under the administrative control of Industries & Commerce Department of the Govt. of Assam.

G. The company has grown organically over the last 57 years and moved from one bulk consumer to 30,000 domestic, 10,000 commercial consumers, 400 industrial consumers and a few power, fertilizer and petrochemical bulk consumers. To cater the changing needs, the systems, processes and control mechanism have undergone gradual changes. To reflect current business environment and build upon the opportunities and strengths by overcoming the weaknesses, it has become necessary to design integrated managed systems and processes. The systems and processes also requires in-built corporate governance and compliance to statutory rules and regulations.

5.2. Objective of the Project

A. Being a pioneer organization operating in City Gas Distribution (CGD) sector in a dynamic and increased competitive environment, the company realizes the significance of Information Technology (IT) as a strategic business enabler to streamline, integrate and standardize the business processes and the overall operations across the organization. In doing so, the company has embarked upon a major IT initiative to establish datacenter at AGCL, Duliajan to cater to the need of their existing lines of business.

B. AGCL intends to integrate their main business processes, in real time, mediated by software and technology and plans to use, automate, and manage day-to-day business activities such as accounting, procurement, project management, risk management and compliance, and supply chain

operations through greater transparency. Apart from this AGCL intends to establish a redundant, manageable, secure, and next generation network. The network should not be a hindrance in the performance of the ERP solution to be implemented and must be designed to manage and handle futuristic incremental traffic.

6. Pre-Qualification Criteria (PQC)

6.1. Eligibility Criteria for Bidder- ICT Infrastructure- SI

S.No.	Criteria	Mandatory Documents to be submitted.
A.	**Organizational Parameters**	
1	Bidder should be a registered Proprietary firm or partnership firm or private or LLP or Ltd. Company and a company incorporated in India under the Companies Act, 1956/Limited Liability Partnership Act 2008 and subsequent amendments and should be in existence for the last 8 years as on the date of issue of NIT in the areas of supply, implementation, operation and maintenance of Data Centre related ICT Infrastructure solution for large integrated solution such as ERP.	Certificate of Registration/ Certificate of Incorporation for the mentioned criteria must be provided by the bidder, self-attested by the authorized signatory of the bidder.
3	A power of attorney / Board resolution in the name of the person signing the bid by Bidder	Power of attorney/Board resolution copy
4	Should have valid PF, IT, GST Registration Certificate.	All the supporting documentary evidences for the mentioned criteria must be provided by the bidder, self- attested by the authorized signatory of the bidder.
5	The Bidder should be an OEM certified/authorized System Integrator/Implementation Partner for the proposed Core ICT Infrastructure Hardware and Software Products. The System Integrator/Implementation Partner should have valid authorization/certification from the respective OEM(s) and have active relationship with the respective OEM(s). OEMs Authorization for Servers, Network equipment, Storage, Backup Solution, EMS, etc., are to be submitted.	Required Certificate(s)/Authorization(s) from the OEM(s) have to be submitted in Annexure 5. [Note:- The Annexure 5 should be filled and submitted separately for each OEM]
6	The Bidder should have an Average Annual Turnover of Rs. 150 Crore or more for last three (3) financial years ((FY 2017-18, FY 2018-19, FY 2019-20) with positive Net Worth for each of last three (3) financial years (FY 2017-18, FY 2018-19, FY 2019-20) from IT/ ITeS services / supplies	Audited Annual Accounts for last 3 years (FY 2017-18, FY 2018-19, FY 2019-20) along with duly filled in Annexure 3. Audited Annual Accounts Statements (Relevant Schedules and Annexures, Statement of Asset and Liabilities & Profit and Loss Account) indicating the Annual turnover of the bidder from ICT Infrastructure solution selling and its implementation in last 3 years (FY 2017-18, FY 2018-19, FY 2019-20) should also be submitted. Positive net worth certificate certified by chartered accountant also needs to be submitted by the bidder.

S.No.	Criteria	Mandatory Documents to be submitted.
7	Any direct Contract Agreement of the proposed bidder for ICT Infrastructure with AGCL should not have been terminated in last five (5) years.	Self-Declaration/Certification by the authorized signatory of the Bidder in the attached Annexure 18.
8	The Bidder shall not be under declaration of ineligibility for corrupt or fraudulent practices or blacklisted or debarred in last five years by any Department / Agency / PSU/ Organization of the Government of India or any State Government in India for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices.	Self-Declaration /Certification by the authorized signatory of the Bidder in the attached Annexure 4.
9	The Bidder should hold a valid ISO 9001:2015, ISO/ IEC 20000-1: 2011 and ISO 27001:2013. The certificate should be valid as on the date of submission of the bid	Copies of the required valid certifications to be submitted.
B	**Human Capital Strength**	
1	The Bidder should have on its own payroll at least 150 technically qualified ICT Infrastructure professionals for providing technical services related to supply, installation, testing & commissioning followed by operation & maintenance of Data Center ICT Infrastructure, other ICT Infrastructure and associated packaged software, etc., out of which at least 30 employees should have minimum three (3) years of experience of working in data center environment and experience of successful implementation, operation and maintenance of data center ICT infrastructure including servers, Backup Solution, Data Center Networking, EMS Solution, etc.	Certificate from firm's HR department to be submitted duly self-attested by the authorized signatory. Annexure 19
2	The Bidder should have a well-established presence in India with a support base to provide implementation and support for the proposed ICT Infrastructure solution & services along with the ability to provide timely response and service to the owner.	Declaration letter signed by the authorized signatory of the Bidder along with adequate documentary evidences in respect of submission to be enclosed.
3	The Bidder should have a point of presence in the state of Assam or should open a Project Office within 30 days of receipt of Letter of Intent (LoI).	Relevant document proof for presence in state. OR An undertaking to this effect should be submitted by the bidder on its letter head.
C.	**General**	
1	The ICT Infrastructure solution- hardware OEM(s) whose products have been offered in the bid should be a registered firm or a company in India and should be in existence in India for last five (5) Years in the areas of selling of Data Centre related ICT Infrastructure solution(s), other ICT	All the appropriate supporting documentary evidences for the mentioned criteria must be provided by the ICT Solution Implementation Bidder.

S.No.	Criteria	Mandatory Documents to be submitted.
	Infrastructure and associated packaged software, etc.	
2	The Bidder should submit valid authorization letters from each of the OEMs of the offered ICT Infrastructure related Product confirming that the products meet the technical & functional requirements asked for in the RFP document and that the Products quoted are of latest version / specification and are not at the end of sale, end of life and end of support.	OEM's confirmatory letters to be enclosed by the ICT Infrastructure Implementation Partner (bidder), along with duly filled up [Annexure 5] [Note:- The annexure should be filled and submitted separately for each OEM]
3	The offered products and the OEMs of any of the offered products should not be under declaration of ineligibility for any cyber security or information security threat by any Sovereign Government.	Self-Declaration /Certification by the authorized signatory of the Implementation Partner (the Bidder) along with self-declaration of the authorized signatory of the respective product OEMs in the attached Annexure 18. [Note:- The Annexure 18 should be filled and submitted separately for each OEM]
D.	**Implementation Experience**	
1	The Bidder should have should have executed at least 1 project for IT Data Centre Implementation/ Maintenance with any Government / PSU Organization in India in last 5 years as on the date of submission of the bid: i. One similar project having the ICT Infrastructure component of total value of at least Rs 8 Cr (Eight Crore), OR ii. Two similar projects having the ICT Infrastructure component of total value of at least Rs 4 Cr. (Four Crore) each, OR iii. Three similar projects having the ICT Infrastructure component of total value of at least Rs.3 Cr. (Three Crore) each. Note:- Similar on-going/under implementation ICT Infrastructure projects shall be considered only in such cases where at least delivery and installation of the ICT Infrastructure for the required value have been completed.	All the appropriate supporting documentary evidences for the mentioned criteria must be provided by the ICT Infrastructure Implementation (the bidder). The satisfactory performance certificate should be in the form of:- • Work Order + Completion Certificates from the client; •For on-going/under implementation projects where Phase Completion Certificate from client are not available however the delivery and installation of the ICT Infrastructure for the required value have been completed then, Delivery challan of ICT infrastructure delivered along with Work Order + Certificate from the client regarding completion of delivery and installation of the ICT Infrastructure of required value should be submitted, clearly mentioning the complete scope of work under the Order and the total project value. Bidder shall have to provide access to the Owner/ Consultant (within 7 days of request from the Owner/ Consultant) for validation from the customer's authorized signatory (including valid contact details) so as to enable the Owner to verify such information as required above. Bidder shall also submit the Annexure 8 along

S.No.	Criteria	Mandatory Documents to be submitted.
		with aforesaid documents
2	Bidder should have executed or in the process of executing at least 1 ICT project of value Rs. 4 Crore with any Government Organization in North Eastern State in India in last 5 years as on the date of submission of the bid.	All the appropriate supporting documentary evidences for the mentioned criteria must be provided by the ICT Infrastructure Implementation Partner (the bidder) in the form of:- • Work Order / PO Bidder shall also submit the Annexure 8 along with aforesaid documents

	c. Mandatory Professional qualification: - Certification in PMP/ PRINCE2	Copies of certificates to be provided

Note:

A. All self-certificates and documents must be digitally signed using digital signature, and physcailly signed, sealed and dated, by the Authorized signatories of the Implementation Partner (the Bidder), unless specified otherwise.

B. Internal implementation including implementation in subsidiary companies of the bidder will not be considered as required qualifying credentials.

C. The Bidder should have the credentials to meet all of the above mandatory criteria to become eligible. In case any of the conditions listed above is not met, the Bidder will be disqualified. Only proposals which meet all of the above Pre-qualification requirement would be considered further for techno commercial stage.

6.2. Eligibility Criteria for OEM

A. The OEM must be present in India since more than 7 Years

B. The OEM must have its spare depot in Guwahati/Kolkata either owned or through its Authorized Distributors / Partners. A written undertaking in this regard must be submitted by OEM duly signed and stamped and the same shall be submitted as an annexure to total responsibility annexure submitted by bidder/SI

C. The OEM must submit in writing that Product being Quoted are not EOL (End of Life) and EOS (End of Service) and they will provide comprehensive warranty support for a minimum of 5 years and desired up to 7 Years from the date of Go-live / as per Terms of the Contract

D. All Warranty of the equipment's must start from the date of Go-live or 200 Days after the date of delivery at-site whichever is later. The warranty under this RFP is a comprehensive onsite warranty for the entire solution including all the equipment installed.

E. The OEM will authorize only Tier-1 or highest status level Partners /or who have at least 5 dedicated and certified personnel on their product line with them since at least last 3 Years. The written undertaking in this regard must be submitted duly certified, stamp and signed.

F. The OEM/SI must certify that solution being supplied is covered with proper warranty packs, and the models being quoted are fully complied in-line to Technical Specifications as asked for in the RFP.

7. Technical Evaluation Criteria (TEC)

A. The solution offered by the bidder should be in 100% compliance with all the technical specifications as mentioned in the section "Core ICT Infrastructure-Scope" and "Hardware Sizing" of this RFP which is mandatory and bidder should ensure to provide the complete ICT Infrastructure to AGCL formeetingthetechnicalrequirementfor hosting ERPasspecifiedtherein. Non- compliance to any of the technical requirements as specified in the section "Hardware Sizing" and "Core ICT Infrastructure-Scope" along with the other sections of this RFP would result in disqualification of thebid.

7.1. Selection Methodology

A. The evaluation committee will evaluate each of the bids on the basis of L-1 Evaluation criteria. At the stage of evaluation, the financial quotes from pre-qualified bidders and 100% Technical compliant are evaluated and lowest bidder will be selected.AGCL will/may ask all Qualified Bidders for technical presentation and understand the solution and implementation approach. AGCL TEC will have all rights reserved to disqualify any bidder basis poor understanding of the scope and non-capability of the SI to implement the solution. All participating SI/bidder must have Qualified team as asked in the Eligibility Criteria.

B. AGCL reserves the right to ask for additional information/clarification (if reqd.) for the evaluation of bids. Bidders that fail to submit additional information or clarification as sought by evaluation committee, their bids will be evaluated based on the information furnished along with the bid proposal and may also be summarily rejected if found to be deficient as per the terms and conditions of this RFP

8. Scope of Work

8.1. Hardware Scope

A. Bidder shall set up an IT datacenter at the premises of AGCL in Duliajan, Assam. The deployed architecture shall conform to the hardware sizing requirements as provided under Section-Hardware Sizing which shall be verified by the bidder. The scope requirements of AGCL in context of setting up the Data Center is as below:

B. The System Integrator shall be responsible for supply, installation, configuration, Testing and commissioning of Core ICT Infrastructure, as per the RFP, for hosting the proposed ERP system of AGCL at AGCL data center, Duliajan, Assam.

C. The System Integrator shall ensure that adequate skilled technical and qualified staff is available to operate and manage the DC infrastructure of AGCL at desired levels, as per the RFP.

D. The recommended servers should be able to accommodate possible scaling up requirements in the future. All hardware including, but not limited to, the servers procured shall be branded and reputed.

E. The contractor shall submit validation from all Hardware OEMs as part of their bid for the products that have been proposed in the ERP system certifying that solution proposed by the bidder is relevant and adequate with respect to their respective product(s).

F. Detailed Scope of Work regarding Core ICT Infrastructure is given in Section 9- Core ICT Infrastructure Scope.

8.2. Project Governance Structure & Reporting

A. In order to ensure better monitoring and control of project the formation of following committees is needed before commencement of the project. The structure of these committees will be:

B. Steering Committee – This committee will consist of the top management employees of AGCL, PMO consultant representative ,Datacenter Project Director of the SI. The Steering committee would provide guidance from a strategic perspective and will perform monthly review of the project progress and issue or dispute resolutions, if any.

C. Project Management Committee (PMC)– This committee consists of Project Director, Project Manager, Training Manager both from SI and AGCL. The PMO would be responsible for operational management of the Datacenter project, such as ensuring adherence to the project plan and management of deliverables and project resources. The PMC would also enable communication and reporting across the project organization, including the project team and senior management.

D. PMO: AGCL will have their own project manager for the Datacenter project. The SI is also expected to appoint a dedicated full-time project manager. Additionally, AGCL will appoint a third-party Project Management consultant for oversight and monitoring of the project. These above roles will jointly form the project management office (PMO) and work closely with each other.

E. Core Group (Core Team) – This group consisting of Functional Experts, technical experts and infrastructure experts of SI and AGCL

F. Project Reporting - The SI shall provide weekly and monthly progress reports. The formats and contents of the weekly and monthly progress reports will be finalized at the start of the planning phase and shall be jointly agreed by AGCL and SI. The formats shall cover but not limited to the following:

i. Progress against the Project Management Plan in terms of activities and deliverables

ii. Status of all risks, challenges and issues, and the related mitigation activities

iii. Status of testing at applicable stages of the project

iv. Exception reports

v. Issues that require action along with proposed effective solutions and persons responsible therefor.

vi. Timelines for implementing such solutions to remedy such issues.

G. Weekly review meetings shall be held at AGCL premises and shall be attended by the designated Project Manager and senior staff of the SI. Other than the planned meetings, AGCL may also call for Steering committee/Project Management Office group meeting with prior notice.

H. AGCL reserves the right to ask the SI for the project review reports other than the standard weekly review reports.

I. AGCL reserves the right to ask the SI for the project review reports other than the standard weekly review reports.

8.3. Core ICT Infrastructure- Scope

A. The contractor shall be responsible for the complete Design, Supply, Installation, Configuration, Testing and Commissioning of the Core ICT Infrastructure solutionfor implementation of proposed ERP Solution in AGCL as per the RFP. Indicative list of key activities which need to be performed by the contractor or its implementation partner in respect of ICT Infrastructure to be implemented under this RFP are as given below, but the list shall not be limited to these:-

a. Project Management for the entire project from commencement to final handing over for live use

b. Information exchange and planning for the project with AGCL.

B. Best practices and standards prevalent for Data Centre has to be adhered while designing. The project is 'Turn-key' type in true sense. The successful bidder has to execute the project with accordance to the detailed scope as mentioned in the RFP.

C. The solution shall comprise of supply, installation, testing, commissioning training and handing over of all materials, equipment, hardware, software, and necessary labor to commission said system complete with all the required components strictly as per (but not limited to) the latest codes.

D. The bidder shall provide detailed design, documentation, make, and model, efficiency including user, system and operation manuals along with the necessary diagrams, design drawings and details bifurcation of Bill of Quantity (BOQ) along with detailed description. The shop drawing (to be submitted before execution or as on when required) may include but not limited to the following as mentioned in the BoQ:

- Site layout
- Equipment placement layout
- All drawing for Electrical scheme including single line diagram
- All GA drawing of equipment

- Piping schematic
- Grounding and Earth pits
- Network cabling

E. The bidder shall be responsible for performing verification tests at their factory and at site to ensure all proposed software and hardware are functioning as per design at their own cost.

F. The bidder shall take the necessary clearance / approval of the drawings, design, quality of material, make and model of the quoted material etc. prior to the execution of the project

G. The bidder shall perform necessary site survey to understand the business context and detailed requirements of AGCL under this RFP.

H. FAT/ UAT and Audit of installed solution before Go-Live. Go-Live will be limited to Installation, configuration of all but not limited to HCI Nodes, Security devices, SDN Devices, Smart Rack, UPS, Passive work and all listed equipment's as per details mentioned in PO to ICT SI/Bidder. AGCL will ensure availability of RAW Power, Genset, Internet Bandwidth at all respective offices being covered in the scope.

I. Preparation and submission of all necessary documents required during various phases of the project, viz., planning, design, installation, commissioning, rollout, acceptance testing, etc. shall be carried out by bidder

J. Warranty of the ICT Infrastructure for a period of Five (5) years, from the date of Enterprise Wide Go live shall be done by bidder

K. Training: The bidder shall identify/ select and subsequently impart operational training to AGCL's identified IT/Technical personals (around 20-30 nos.).

8.4. Information exchange, Site Surveys and Planning

A. System Integratorwill conduct necessary studies including site surveys of AGCL location under the scope of this RFP to understand the overall network architecture and the services being provided by AGCL for implementation of GCCS and LAN Solution and the Primary WAN Service Provider so as to effectively use that information while designing the ICT Infrastructure solution/Datacenter under this RFP.

B. For performing site surveys of AGCL locations, the Contractor shall have to submit proposed site visit plans and travel plans including team details, well in advance, for AGCL's approval and necessary coordination. System Integratoragainst this RFP shall also provide a detailed communication plan to exchange information with the implementation agency appointed by AGCL for its GCCS & LAN Solution and the WAN Service Providers (Both primary and secondary).

C. It is the responsibility of the System Integratorto perform detailed site surveys and studies to assess as accurately as possible and come up with detailed solution as per the requirements given in this RFP. AGCL will provide plant layouts, diagrams, etc., to the extent available and the bidders are advised to obtain all the other required information by performing site surveys. Bidder shall submit detailed Site Survey reports as part of the proposed ICT Solution Document/ICT Solution Design Document (as explained in subsequent section).

D. The System Integrator will perform study of existing/proposed network infrastructure. Following is the indicative list of information that might be exchanged with AGCL forLAN solution and the WAN Service Provider(s):-

i. Position of network ports at each location or locations for installation of end user computing equipment.

ii. Possible integration methods for exchanging information in automatic fashion between GCC application and ERP Solution.

iii. High Level security architecture (excluding configuration of security and network devices).

iv. Transmission port numbers to be allowed for functionality of ERP, DMS and other applications and services.

v. IP address required to be assigned to end IT equipment and datacenter equipment. The bidder may please note that the IP schema will be designed by the implementation agency appointed by AGCL for LAN Solution. The successful bidder against the instant RFP shall coordinate with the implementation agency selected under the LAN Solution and GCCS Solution for ensuring a seamless and efficient ICT infrastructure of AGCL under the Project

vi. WAN bandwidth and performance information.

vii. Other technical information for effective designing and functionality of overall solution.

E. The above-mentioned list is indicative in nature and the final list of information and details to be exchanged will be agreed during the coordination meetings to be held between AGCL, the agency appointed by AGCL, once the successful bidder against the instant tender is on-board with AGCL. Under all circumstances the contractor would be required to take prior approval from AGCL before exchanging information with the other service providers of AGCL. Similarly, the System Integrator will ensure that the confidentiality and integrity of the information exchanged is upheld and there is no breach/ leak of confidential information. It will be the selected bidder's responsibility to ensure that documents and the information collected during the site surveys are kept confidential and are not misused in any way.

8.5. OEM Certificate of Equipment

A. In case the spares and warranty are supplied by the authorized supplier of the OEM, then if the authorized supplier fails to repair/ maintain the equipment during the comprehensive warranty, the responsibility for maintenance of the equipment provided would then be taken over by the OEM.

B. The complete contact details of the OEM (Name and designation of contact person, postal address, e mail ID and telephone & FAX numbers) will be furnished and the buyer may at his discretion verify the authorization from the OEM, failure of which may result in the bidder being black listed and / or barred from participating for any future tender of this organization.

8.6. Spares and Equipment Performance

The Successful Bidder shall stand guarantee for the supply of spares of all the equipment under the scope of supply for a minimum period of 5 years from the date of awarding the contract and also guarantee that discontinuity of production of any item offered as a part of the system shall not affect the maintainability of the system for a period of 5 years from the start date of operation and maintenance support of data Centre.

8.7. Key Design Considerations

8.7.1. Scalability

A. A scalable system is one that can handle increasing numbers of requests without adversely affecting the response time and throughput of the system.

B. The Data Centre should support both vertical (the growth of computational power within one operating environment) and horizontal scalability (leveraging multiple systems to work together on a common problem in parallel).

C. Modular design of the Data Centre is an excellent strategy to address growth without major disruptions.

D. All components of the data Centre must support scalability to provide continuous growth to meet the requirements and future demand from various existing or new departments.

E. A scalable Data Centre shall easily be expanded or upgraded on demand. Scalability is important because new computing component is constantly being deployed, either to replace legacy component or to support new mission.

8.7.2. High Availability

A. Designing for high availability assumes that systems will fail, and therefore the systems are configured to mask and recover from component or server failures with minimum application outage.

B. All components of the data Centre must provide adequate redundancy to ensure high availability of the applications and other Data Centre services.

C. The Bidder shall make the provision for high availability for all the services of the data Centre.

D. Application availability is the responsibility of the application owner and the Bidder cannot be held responsible for any problem related to application and its availability.

8.7.3. Interoperability

A. The entire system/ subsystem should be interoperable, in order to support information flow and integration.

B. Operating systems and storage technologies from several vendors must interact well with each other. These systems should also support the open architecture solutions where information/ data can be ported to any system, whenever desired.

8.7.4. Manageability

A. The Data Center must be designed in an efficient way to ensure an ease in maintenance.

B. It must facilitate ease of configuration, ongoing health monitoring, and failure detection that are vital to the goals of scalability, availability, and security.

8.7.5. Cyber Security

A. The Data Centre must provide an end-to-end security blanket to protect applications, services, data and the infrastructure from intentional, unintentional or malicious attacks or theft from external (through internet) and internal (through intranet and or physical) hackers/malicious intent.

B. Such attacks and theft should be controlled and well supported using next generation cyber security appliances e.g. Firewalls, IPS, WAFsystems and infrastructure protection mechanisms.

8.7.6. Design Validation and Change

The successful Bidder would be required to prepare detailed deployment design document and shall submit the same for approval within 2 weeks from the signing of the contract Agreement with AGCL. However a Solution design has to be provided during the bid process.

8.8. Installation and Configuration of the IT Infrastructure

A. The successful Bidder would be required to undertake pre-installation planning at the Data Center including but not limited to civil design, Construction, Rack planning if required , structured cabling, cabling, power points, etc.

B. The Bidder shall be responsible for the delivery, installation testing and commissioning of the servers, storage, network, security etc. and related equipment in the Data Centre/Site Offices.

C. The Bidder shall carry out the planning and layout design for the placement of equipment in the provisioned Data Centre. The plan and layout design should be developed in a manner so as to optimally and efficiently use the resources and facilities being provisioned at the Data Centre/Site Offices.

D. The plan and design documents thus developed shall be submitted to AGCL for approval and the acceptance would be obtained prior to commencement of installation.

E. The Bidder shall carry out installation of equipment in accordance with plans and layout design as approved by AGCL

8.9. Deployment Phase

A. Bidder should be involved in Planning, Designing, and final acceptance to make sure that proposed solution should work seamlessly as per tender requirement. The SI shall procure the materials and equipment as required and given as part of the SI's response.

B. After successful commissioning and FAT completions of the project, bidder to ensure complete handover and knowledge transfer to AGCL/ ERP Solution Provider

C. The seamless integration of all IT and Non-IT devices would be the bidder's responsibility holistically.

8.10. Procurement and Delivery of IT Infrastructure Components

A. The Bidder shall procure and supply all components and subcomponents (Active as well as passive), as per requirements of the RFP/Contract. The Bidder shall be responsible for supply/ installation of:

B. All active and passive components required for the Datacenter

C. IT Infrastructure components such as Storage, Networking & Security components and other IT components required at the Data Centre

D. The SI will be responsible for delivering the equipment at the data Centre site. The SI shall supply all the installation material/ accessories/ consumables (e.g. screws, clamps, fasteners, ties anchors, supports, grounding strips, wires etc.) necessary for the installation of the systems.

E. It will be the responsibility of bidder to deliver civil and construction work for setting up of datacenter.

F. The SI has to prepare and submit a delivery report including details of all components supplied. The delivery report will be validated by the AGCL.

G. Any additional equipment procured by Bidder, will be supplied by the respective OEM. The Bidder would be responsible for inventory check, testing and installation of the equipment accordingly and coordinating with the supplier as required.

8.11. Implementation

A. Bidder shall provide a complete data Centre solution to AGCL as a part of their technical bid. Any activity not mentioned here but required for the implementation of data Centre shall be taken in note.

B. The solution provided by the Successful Bidder shall meet all the service level requirements.

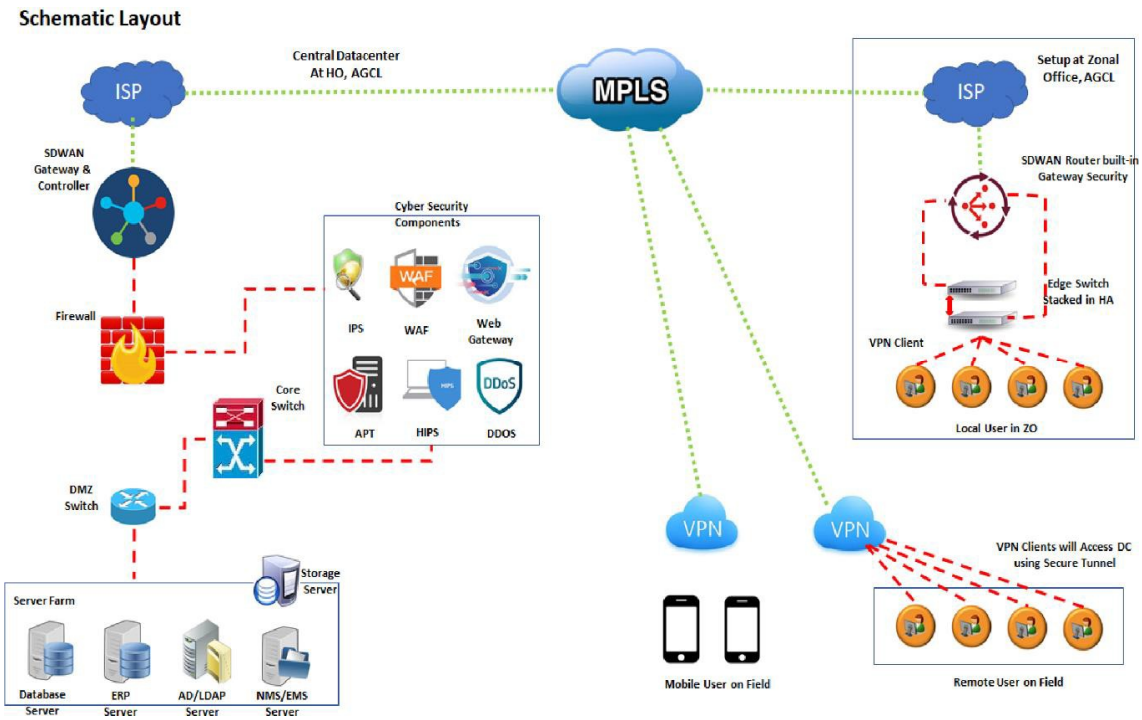
C. Bidder shall be responsible for complete management of the project as per RFP T&C.

D. Bidder to ensure that the entire infrastructure is supported back to back by respective OEM's support services.

E. Solution Capability: The professional experts from the SI / OEM team are expected to support in periodic reviews during the project timeline to ensure that capabilities of the proposed infrastructure are deployed effectively. The reviews are expected to take place at the following stages of the project implementation.

- Technical Solution Preparation
- Solution Implementation
- Final Preparation for Go-Live
- Stabilization period
- Final Go Live.

8.12. Hardware Sizing (Including Technical Specifications and BoM)



A. The Datacenter will be setup at AGCL, HQ in Duliajan. The DC being proposed will cover the following aspects – (pls. Annexure for detail specifications)

B. The DC will be setup using Smart Rack Solution – with built in Cooling, Power, Access management.

C. The DC room will be approximately 1000 Sq. Ft and the battery room will be at least 150 Sq. Ft

D. The Electric panel room has to be proposed in the Battery room and adequate Cabling has to be supply, install, and commissioned by the selected SI.

E. The Smart Rack solution must have built-in Rodent, Surveillance, and Fire Safety devices

F. The Smart Rack all devices must be SNMP based so that same can be managed through Centralized EMS Solution.

8.12.1. Key Provisions Being Made by AGCL

A. AGCL will provide dedicated MPLS network or with multiple links like Broadband, RF, LL available in the State of Assam wherever possible for connecting various offices

B. AGCL will provide One 3-Phase Raw Power Source from the main Grid

C. AGCL will provide Diesel for the Gensets for the Datacenter

D. AGCL will provide Seepage free room on either Ground Floor or 1st Floor to safeguard the proposed Datacenter filling with water logging

E. AGCL will provide all required permissions from the local authorities, internal departments for laying of Fibre, right of way, road cutting, digging trenches etc., if required

F. AGCL will permit the SI to work after Office hours, public holidays, Saturday & Sunday so that timely work can be completed.

G. AGCL will provide lockable room for storing SI material, tools, sitting place for manpower

H. The SI will have to validate and provide his inputs on the below hardware/design specifications.

8.12.2. Details of the Proposed design:

The AGCL Datacenter will host the ERP and other applications to be used by AGCL and its employee to run their business operations. The proposed solution has been considered keeping in view the best practices adopted in the Industry. The solution considered will ensure performance, future upgradability, Secure network, and ease of centralized management.

The salient features of the data center which will be set up by SI on behalf of AGCL and provided to ERP SI are as below:

A. The Datacenter will be hosted at AGCL, HQ, Duliajan, Dibrugarh, Assam

B. The room size which will be provisioned for establishing the Datacenter will be max 1000 Sq. Ft and UPS Battery, Electric Panel room will be separate and will be approx. 150 Sq. Ft.

C. The Datacenter will be established using SMART RACK ENCLOSURES and all devices being proposed must be SNMP ready from Day 1. Pls. refer the detail specifications as mentioned in Annexure

D. The PAC, UPS will be supplied and installed in HA mode.

E. The AGCL network will be setup on the Next Generation SDWAN technology. The SDWAN Controller will act as the Gateway device wherein multiple ISP Links will be terminated. Pls. refer detail specifications as mentioned in Annexure

F. The Firewall will be the Gateway Security and network will be installed and monitored through various security devices like WAF, DDOS, Web Security Gateway, Advance Persistent Threats and all of these logs must be monitored through SIEM solution for further analysis. Pls. refer specifications as mentioned in Annexure

G. The Hyper Converged Infrastructure – a Software defined unified system that combines all the elements of a traditional data center: storage, compute, networking, and management. The DC will host the HCI nodes and Storage wherein the related Applications and ERP Software will be hosted.

H. The LAN at the HQ will be a 3-Tier architecture.

I. The SI will be required to establish an Identity Manager integrated with AD/LDAP for centrally managing the authentication of identities and authorization policies to access the DC by the authorized, Guest Users.

J. The SI will enable DHCP enabled network all across the AGCL. Automatically DHCP Server should assigns IP addresses, default gateways and other network parameters to client devices.

K. The SI will be required to prepare IT Policies, Cyber-security policies along with AGCL and ensure they are applied and followed.

L. All logs must be maintained, and any threats should be mitigated.

M. SI must install and configure Application security tool to encompass measures taken to improve the security of an application often by finding, fixing, and preventing security vulnerabilities in the Codes.

N. The SI must install Database Security tool controls, and establish measures designed to confirm and preserve database confidentiality, integrity, and availability. It must need to protect data: first, from accidental loss and corruption, and second, from deliberate unauthorized attempts to access or alter that data

O. SI must place technically qualified personnel to manage the DC and DR network. The personnel will be available 24x7, 365 Days.

P. All personnel at AGCL, HQ will access the required Applications and ERP basis their role and as authorized.

Q. All the Zonal Site Offices (ZO) will have SDWAN device with gateway Security enabled and basis this the Local LAN will be established.

R. All Passive work which is necessary for enabling the commissioning of Datacenter including civil work and others will be executed by the appointed SI.

S. All personnel at AGCL, ZO will access the required Applications and ERP basis their role and as authorized.

T. The Key backbone in the DC will be 10G among all devices and all users on the LAN will be 1G. Pls. refer the detail specifications as per Annexure.

U. The SI in consultation with AGCL IT team will be required to prepare policies for enablement of DLP & EMAIL Security policies.

V. The SI will enable Proxy solution to monitor the Web usage and access policies.

W. The MS-Exchange (Mail Server) of AGCL will also be hosted from the DC at AGCL, HQ

X. The DR Site will be hosted by the SI at any ISP or CSP in consultation with AGCL. The decision of the same will be taken later. AGCL may prefer to use DR over Cloud through any establish CSP like – Azure, Google, AWS etc.

8.12.3. Technical Specification

The SI shall have to provide AGCL the hardware as per below Technical Specifications to ensure performance, future upgradability, Secure network, and ease of centralized management. The same will be used by ERP System Integrator for hosting ERP Application. The ERP SI will have to provide its inputs on the sufficiency of Proposed Design/Hardware based on his Assessment of below Technical Specifications.

Hyper Converged Infrastructure (HCI) (For Production & Test Environment of the ERP and Other Applications

Technical Parameter/Standard
HCI solution should be in leader's quadrant by latest Gartner Report for Hyperconverged Infrastructure
HCI solution should be implemented at least five customers in India across any Govt. Organization/PSU's with more than 10 nodes cluster successfully implemented
HCI solution should have their at least one support center in India (Hindi supported center) and it should be operation from last five years
HCI solution should have at least five published case study for India customer's available on their public domain
HCI solution should also be available publicly (at no cost) to host qualified hardware without OEM support for testing.
HCI solution should support for hosting their SDS (Software Define Storage) component with choice of server's hardware available from leading OEM's/ODM's
Solution must be proposed with at least 6 nodes in the cluster. Out of these 6 nodes, 2 should be dedicated to run Production DB, and must have dual 26 core processors and 2 TB RAM. Other nodes will host all other applications for Production, Quality and Development. These nodes must have at least dual 16 core processors and 512GB RAM. Offered HCI nodes must be All-flash and must have caching on at least 4 disks in each node. Offered solution must provide 60TB usable capacity, without considering any data efficiency tools, like deduplication, compression and ensure coding.
HCI solution should support more than one hypervisor with cloud native integration (Container)/Openstack
HCI solution must have a feature of exporting the Block LUN to a physical server outside the HCI cluster.
HCI Solution must support two node failure from day one. Offered solution must have selective choice of one additional copy of data for certain VM's & two additional copies of data for other VM's.
HCI solution should support NVMe, SSD, SAS & NLSAS disks without compromising any of enterprises storage efficiency provided by stack
HCI solution must have capability to support HCI nodes with different models (same OEM)/different CPU, Memory & Disks configurations in the same cluster without any impact on enterprise-class storage services/functionalities
HCI solution must support having server and storage nodes with high performance GPU capabilities in a single cluster, seamlessly, with no downtime to scale performance and capacity on demand. HCI must also support live migration of VM with GPU.

Technical Parameter/Standard
HCIsolutionshouldsupportforrack&chassisawarenesstosupportredundantdatashouldgotodifferent rack, chassisnodes
HCI solution must provide on the fly change of ESE (Enterprise Storage Efficiency)-Deduplication/Compression for workload without any visible impact on storage and theiroperations
HCI solution must support ESE (Enterprise Storage Efficiency) (Deduplication, Compression and Erasure Coding) across specific workload and across all tier of storage disks in cluster
HCI solution must have capability to add All flash nodes to the same HCI cluster in the future. If this is not supported, the bidder must propose all-flash HCI cluster from day 1
HCI solution should support security compliance for at least three or more industry certification (CCC-Common Criteria Certified, FIPS-140-2, ISO-27000(ISMS), NIST Guideline for Standard security template (PCI-DSS)/HIPAA etc.
HCI solution must support two copies of data across cluster and should have capability for supporting three copies for critical data and it should be available on workload level.
HCI solution should support data replication across sites with 5 - 10 min RPO and grouping of Virtual machines as per application architecture
HCI solution should support WAN Bandwidth optimizer along with defined schedule across two sites and only increment data should be replicated post one-time data sync
HCI Solution should support one view for physical and virtual network along with their real time usages and configuration
HCI solution should integrate with L2/L3 network device with API call function for all required network configuration(L2/L3) with VM Life cycle
HCI solution should support 802.1Q standard for network Quality of Service
HCI solution should support leveraging external physical servers' access to HCI storage using native ISCSI with highly available connectivity using HCI native load balanced and distributed data architecture across all nodes in cluster
HCI solution should support natively Microsoft and Linux based Guest VM's Clustering using block storage
Solution must have scale-out architecture for linear capacity and performance enhancement. The solution must be able to enhance cluster capacity and performance whenever required with recommendation
Solution should support native file storage supporting NFS v3/v4 and SMB 2.0/3.0 for Linux and Windows Guest with unlimited shares integrated with Active directory/LDAP

Technical Parameter/Standard
Solution should support integrated File Storage should support native scale-up and scale-out distributed architecture file storage with session load balancing functionality for consistent user session
Solution should support integrated file storage should support user and group level share quota restriction with hard and soft limit
Solution should support integrated files storage must restrict users to see any other files/folder other than their designated permissible files/folders
Solution must support in-built File Analytics, and monitor the consumption on the basis of files & users
Solution must analyze the distribution of files based on the file-size, file-age & its access pattern.
Solution should have capability for Administrator to search for the filename and record the details of activities on that file in the past.
Solution should be able to define the anomaly rules on the File servers and report any anomalies to the defined administrator through email alert.
HCI solution should provide all key operation management and performance management from a single console for Hardware/Storage/Hypervisor and VM 's management using HTML 5 internet browser
HCI solution should have analytics on capacity behaviour and should have capability of showing all under and over utilized VM's with their right sizing information after current VM's usages
HCI solution should be capable of creating custom dashboard with reporting as per customer ease and requirements, solution should be able to scan/search objects with advanced search option for faster access to require information for trouble shooting
HCI solution should have capability for finding object anomalies from standard behaviours and report this before major bottleneck for solution.
All proposed hardware and software must be 24 x 7 OEM supported for 5 years and must be enabled from day one.
Solution should provide Virtual Network visibility with application-centric protection from network threats and automation of common networking operations
Solution should be able to integrate with provided orchestration layer and cloud management platforms using programmable REST APIs/OpenFlow/Netconf to provide end to end automation of network and security services.

Technical Parameter/Standard
Solution should integrate with 3rd party physical network & security solutions (or their managers) from leading OEMs using programmable REST APIs/OpenFlow/Netconf/Device packages to provide integration with proposed ToR switches
Solution should offer comprehensive flow assessment, analytics, security groups and firewall rules suggestion for the purpose of implementing micro level segmentation to achieve zero trust security within the datacenter
Solution should provide creation of security groups and security policies/rules based on parameters like virtual machine name/OS type/IP addresses/Security Tags etc.
Solution should provide granular control and governance across VM to VM traffic or VMs pre-defined Group/Department
Solution should Support for layer-2 VLAN for networking and integrated VM IP's Management capabilities

EMS

Enterprise Management System (EMS):
General:
For effective operations and management of IT Operations, there is a need for an industry-standard EnterpriseManagementSystem(EMS).Giventheexpanseandscopeoftheproject,EMSbecomesvery critical for IT Operations and SLA Measurement. Some of the critical aspects that need to be considered for operations of IT setup ofare:
a) Network Fault Management
b) Network Performance Management
d) Server Performance Monitoring
e) Centralized Log Management
f) Centralized and Unified Dashboard
g) Centralized and Customizable Service Level Reporting
h) Help Desk for Incident Management
The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: • Event and Alarmmanagement, • Auto-discovery of the ITenvironment, • Performance and availabilitymanagement • Correlation and root causeanalysis • Service Level Management,notifications • Reporting andanalytics • Automation andCustomization
The proposed solution should have at least 2 deployments (in state/central Government, PSU or Large enterprise) with 10,000 devices being monitored in each of these deployments.
The proposed solution must be featured in Gartner/IDC reports. Documentary proof must be submitted at the time of submission.
Thereshouldbeatightintegrationbetweeninfrastructuremetricsandlogstohavethesingleconsolidated console of Infrastructure & securityevents.

Consolidate IT event management activities into a single operations bridge that allows operator quickly identify the cause of the IT incident, reduces duplication of effort and decreases the time it takes to rectify IT issues.
TheOperatorshouldbeabletopullupsecurityeventsrelatedtoagivenConfigurationItem,fromasingle console which also has NOC events, and use the security events to triage the problem. This way the Operatorgetsconsolidatedsystem/networkeventdetailsandsecurityevents(currentandhistorical)from the same console and save time in troubleshooting / isolating theissue.
The operator should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events
Scalability – The system should be capable of supporting at least 15 thousand network flow per second on single server with capability to capture each unique traffic conversations
The solution shall provide future scalability of the whole system without major architectural changes.
The Solution shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc.
All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring
The solution must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operators right from services to last infrastructure components
Consolidated dashboard of the proposed EMS solution must be able to do dynamic service modelling of all business-critical production services & use near-real time Service Model for efficient cross domain event correlation.
The proposed solution must provide SDK/Rest API for North bound and South Bound Integrations, e.g. Forwarding specific metric data to third party database, Notifications to third party systems such as Jira/ Autodesk/Slack/other similar types
DETAILED SPECIFICATIONS: EMS
Consolidated Dashboard
The platform must provide complete cross-domain visibility of IT infrastructure issues
The platform must consolidate monitoring events from across layers such as Network, Server, Application, Database etc
The solution should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases
The solution must support custom dashboards for different role users such as Management, admin and report users
The solution must allow creating custom data widget to visualize data with user preferences e.g. Refresh time, time span, background colour, unit conversion
The solution must support multiple visualization methods such as gauge, grid, charts, Top N etc.
The solution should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console
There should be only one dashboard/interface to collected network/server/application/log data after correlation and consolidation across the IT landscape to reduce/correlate number of metrics/alarms
Network Performance Management:
The proposed solution platform shall provide a single integrated solution for comprehensive management of the wired/wireless access, and rich visibility into connectivity and performance assurance issues.
The design functionality shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the- box implementation automating the work required to use OEM validated designs and best practices.
The proposed solution must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.

The proposed solution must provide the complete view of the Topology and network elements. The NMS shall have the ability to include the network elements and the links in the visual/graphical map of the department. The visual maps shall display the elements in different colour depending upon the status of the element. It is preferable that green colour for healthy and amber/yellow colour for degraded condition and red for unhealthy condition is used.
The proposed solution must have suitable system level backup mechanism for taking backup of NMS data manually as well as automatically
The proposed solution must keep historical data at raw level without averaging for minimum of six month
The proposed solution must provide the visual presentation of the Network Element's status and the alarms. It shall also present the complete map of the network domain with suitable icons and in suitable colour like green for healthy, red for non-operational, yellow for degraded mode of operation etc.
The proposed solution must provide Health Monitoring reports of the network with settable periodicity - @24 Hrs, 1 week, 1 month.
The proposed solution must provide the graphical layout of the network element with modules drawn using different colours to indicate their status
The proposed solution must provide calendar view which allows the operator all the schedule activities such as Reports, Inventory scans etc. It shall also allow to define scheduled report for uptime, link status etc.
The proposed solution should have multiple alerting feature to get the notification via email, SMS and third-party systems
The proposed solution must support listening to traps and syslog events from the network devices with retention period up to 6 months.
The proposed solution must support defining the data retention period to control storage
The solution must support custom device template to support Generic SNMP devices
The solution must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
It shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.
Fault Management: -
The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: • Event filtering • Event suppression • Event aggregation • Event annotation
The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
Powerful correlation capabilities to reduce number of actionable events. Topology based and event stream-based correlation should be made available.
The solution must offer relevant remedy tools, graphs in context of a selected fault alarm/event
The proposed monitoring solution should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks.
The Platform must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management

The solution should classify events based on business impact and also allow defining custom severity levels and priority metrics such as Ok, Critical, Major, Down, Info etc with colour codes
The solution should allow creation of correlation or analytics rules for administrators
The proposed solution must provide default event dashboard to identify, accept and assign generated alarms
Log Management: -
The proposed solution must provide a common classification of event irrespective of the log format
The proposed solution must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes for the period of 3 months and allow to extend it to further with additional hardware without any disruption to the ongoing data collection
The proposed solution should provide a minimum log compression of 8:1 for ensuring log compression to reduce overall log index storage space for the raw log format
The log data generated should be stored in a centralized server. The period up to which the data must be available should be customizable.
The proposed solution must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of events through customization of connectors or similar integration
The proposed solution must support log collection for Directories (i.e. AD, LDAP), hosted applications such as database, web server, file integrity logs etc. using agents
The Log receiver or log collection component must store the data locally if communication with centralized collector/receiver is unavailable.
The proposed solution must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product.
The system shall support the following log formats for log collection: Windows Event Log, Syslog, Access Log Data, Application Log data, Any Custom Log data, Text Log (flat file), JSON Data
The solution should be able to collect raw logs in real-time to a Central log database from any IP device including: • Networking devices(router/switches/voice gateways) • Security devices (IDS/IPS, AV, Patch Mgmt., Firewall/DB Security solutions) • Operating systems(Windows 2003/2008,Unix,linux,AIX) • Virtualization Platforms(Microsoft HyperV, VMware Vcenter/VSphere 4.X, vDirector, Citrix) • Databases(Oracle/SQL/MYSQL/DB2)
The collection devices should support collection of logs through Syslog, syslogNG and also provide native Windows Agents as well as Agentless (PowerShell) connectors
The proposed solution must provide alerting based upon established policy
The proposed solution must provide SDK and Rest API to write custom connectors and collectors to pull log and monitoring data from third party system
The proposed solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.
The proposed solution must collect, index the log messages and support full text searching for forensic investigation
The proposed solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.
The solution must provide pre-defined log correlation rules to detect suspicious behaviour
The solution must support real-time and scheduled alerting timeline while creating a log policy to catch specific log pattern
The solution should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose

The system shall have the capability to drag and drop building of custom search queries & reports
The system shall be capable of operating at a sustained 5000 EPS per collection instance. The system shall provide the ability to scale to higher event rates by adding multiple collection instance
Service Desk - Incident Management
The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface
The proposed helpdesk solution should have achieved PinkVERIFY/equivalent certification on at least 6 available ITIL processes (a documentary proof of the same should be provided at the time of bidding).
Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.
The proposed solution should automatically provide suggested knowledge base articles based on Incident properties with no programming
The proposed solution should automatically suggest available technicians based on workload, average ticket closure time assigning tickets with no programming
The proposed solution should tightly integrate with monitoring system to provide two way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts
The proposed system must not create more than one ticket for same recurring alarm to avoid ticket flooding from Monitoring system
Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via web-based console with no programming
The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email
The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team
The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.
The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues
The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type
The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.
The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window
Service Level Reporting:
The solution should provide reports that can prove IT service quality levels, such as application response times and server resource consumption
The system reports should be accessible via web browser and Reports can be published in PDF and csv format
The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
The solution must provide Reports that can be scheduled to publish automatically, or they can be produced on demand

The solution should be able to report in the context of the business services that the infrastructure elements support—clearly showing how the infrastructure impacts business service levels
The solution should provide Business Service Management functionality to track Service quality by logically grouping Network, Server and Application components. The solution should provide correlation between Network, Server and Application to identify the business impact from the specific event or alarm
The solution must provide way to define key performance indicators (KPIs) within the Service Quality report.
The solution must provide SLA measurement to track service quality from both Availability and Performance perspective.
Role-Based access control: -
The solution should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department
The Solution should have way to control and define permission such as read/write for set of devices rather than all the devices for the ease of use.
EMS Other Key Requirements: -
The Solution should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications
The solution should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO
The proposed OEM should possess Quality Management, IT Management security and Application Security Management certifications like ISO 9001:2008, ISO 27001:2013 and ISO 27034:2011.
The proposed Network Monitoring Solution, Help Desk and Asset Management module should be from a single OEM.

SDWAN + Firewall in HA – 2 Nos.

NGFW Specifications
Firewall
The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems
ThePropos edFirewallVendorshouldbeintheLeaders'QuadrantofGartnerMagicQuadrantforNext Generation Firewall.
Firewall appliance should have at least 16 x 1GE RJ45 interface, 8 x 1GE SFP interfaces, 4 x 10G SFP+ interfaces and 2x40 GE QSFP+ slot.
Firewall Throughput should be 70 Gbps
Firewall should support minimum 30 Gbps of VPN throughput
Firewall should support 20000 site-to-site & client to site VPN Tunnels.
Firewall should support minimum 5,000 concurrent SSL VPN users and should be scalable in future
Firewall should support 450,000 new sessions per second
Firewall should support 8 Million concurrent sessions
The solution should support minimum 9 Gbps of NGFW (FW + IPS + AVC) throughput for Mix / production traffic
The solution should support minimum 7 Gbps of Threat Prevention (FW + IPS + AVC + AV/Malware) throughput for Mix / production traffic
The Firewall solution should support NAT64, DNS64 & DHCPv6

NGFW Specifications
The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.
The proposed system should have integrated Traffic Shaping functionality.
The Firewall should have SDWAN feature to support minimum 4 service provider for load balancing at same time in active/active.
The Firewall & IPSEC VPN module shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification.
The proposed system should support
a) IPSEC VPN
b) PPTP VPN
c) L2TP VPN
The device shall utilize inbuilt hardware VPN acceleration:
a) IPSEC (DES, 3DES, AES) encryption/decryption
b) SSL encryption/decryption
The system shall support the following IPSEC VPN capabilities:
a) Multi-zone VPN supports.
b) IPSec, ESP security.
c) Supports NAT traversal
d) Supports Hub and Spoke architecture
e) Supports Redundant gateway architecture
The system shall support 2 forms of site-to-site VPN configurations:
a) Route based IPSec tunnel
b) Policy based IPSec tunnel
The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode.
The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.
Virtualization
The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 5 Virtual Firewall license should be provided.
Intrusion Prevention System
The IPS capability shall minimally attain NSS Certification
IPS throughput should be minimum 12 Gbps for Mix / Production traffic
The IPS detection methodologies shall consist of:
a) Signature based detection using real time updated database
b) Anomaly based detection that is based on thresholds
The IPS system shall have at least 7,000 signatures
IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available
In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked, and the Firewall will continue to operate while the problem is resolved
IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.
IPS signatures should have configurable actions like terminate a TCP session by issuing TCP Reset packets to

NGFW Specifications
each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident
Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
Antivirus / Antimalware
Firewall should have integrated Antivirus solution
The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services:
a) HTTP, HTTPS
b) SMTP, SMTPS
c) POP3, POP3S
d) IMAP, IMAPS
e) FTP, FTPS
The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
Web Content Filtering
The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.
The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
The proposed system shall provide web content filtering features:
a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.
b) Shall include Web URL block
c) Shall include score-based web keyword block
d) Shall include Web Exempt List
The proposed system shall be able to queries a real time database of over 110 million + rated websites categorized into 70+ unique content categories.
Application Control
The proposed system shall have the ability to detect, log and take action against network traffic based on over 2000 application signatures
The application signatures shall be manual or automatically updated
The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions
Data Leakage Prevention
The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.
High Availability
The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component
The device shall support stateful session maintenance in the event of a fail-over to a standby unit.
High Availability Configurations should support Active/Active or Active/ Passive
Logs and Report
The solution should have 8 GB of Hard Drive Capacity for logging and reporting if not please quote separate appliance
Real-time display of information allows you to follow real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic or IM message traffic.

NGFW Specifications
The appliance should support multiple types of report format PDF.
Centralized Management
Should include at least One dedicated Management appliance with 2 x 1G port from day one
The management platform must be accessible via a web-based interface and ideally with no need for additional client software
The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
Centralized Management should provide a central manager to manage the NGFW and SDWAN appliance which should be capable of managing multiple appliances for uniform policy.

WAF – Web Access Firewall

Web Application Firewall Specs
General Requirements:
Web application firewall should be appliance based and provide specialized application threat protection.
Should be ICSA/equivalent Certified
Should protect against application-level attacks targeted at web applications.
Should provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting,
Should provide controls to prevent identity theft, financial fraud and corporate espionage.
Appliance should have unlimited application licenses.
Automatic signature update and install
Should monitor and enforce government regulations, industry best practices, and internal policies.
Performance requirements
Shouldsupport20,000HTTPtransactionspersecond&atleast8,000HTTPstransactionspersecond
Should support 60,000 HTTP concurrent connections
Should deliver at least 150 Mbps of WAF (HTTPs) throughput
Interface and connectivity requirements
Should support 4 no's of 10/100/1000 Interfaces & expandable to another 4 x 1G ports
Should support 200 GB of Storage space
Feature specifications.
The appliance should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode,
Appliance should continuously track the availability of the Servers being protected.
Should have a Web Vulnerability Scanner to detect existing vulnerabilities in the protected web applications.
Should have Data Leak Prevention module to analyse all outbound traffic alerting/blocking any credit card leakage and information disclosure
Provide controls to meet PCI compliance requirements for web application servers.
Should have controls for Anti Web Defacement and provide ability to check the authorized version of the website content.
Should enforce strict RFC compliance check to prevent attacks such as encoding attacks, buffer overflows and other application specific attacks.

Shouldsupportautomaticsignatureupdatestoprotectagainstknownandpotentialapplicationsecurity threats.
WAF should support fail open in case of hardware failure
Should have built in policies
Should support custom signatures
Provide ability to allow/deny URL access
Ability to define different policies for different applications
Ability to create custom attack signatures or events
Ability to combine detection and prevention
Should protect certain hidden form fields.
Must provide ability to allow or deny a specific URL access.
WAF should support Normalization methods such as URL Decoding, Null Byte string, termination, converting back slash to forward slash character etc..
Must support Website anti defacement.
A given user must be enforced to follow a sequence of pages while accessing.
The WAF should support IP Reputation Service and able to provide up to date information about threatening sources.
Support IPv6 for Reverse Proxy deployments and It should also Support IPv4 to IPv6 and IPv6 to IPv4 communication
Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests
It should support scanning for malicious content in uploads along with File upload violations and support integration with APT solution to scan for zero-day malwares.
Auto Learn
Should have the capability to Auto-Learn Security Profiles required to protect the Infrastructure.
Should provide a statistical view on collected application traffic
Policies must be automatically generated from auto learn results
Auto-learn options should be available to tweak and fine tune rules
WAF should continue to provide protection even while in learning mode.
Brute Force
Should have controls against Brute force attacks
Should Detect brute force attack (repeated requests for the same resource) against any part of the applications
Custom brute force attack detection for applications that do not return 401.
Protection against SYN-flood type of attacks
Cookie Protection
Should be able to protect Cookie Poisoning and Cookie Tampering.
Strict Protocol Validation
Must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP1.1
Should support restricting the methods used.
Should support restricting the method exceptions.
Should validate header length, content length, Body length, Parameter length, body line length etc..
SSL
Appliance should be able to terminate SSL
Should Passively decrypt SSL
Client certificates should be supported in passive mode and active mode.

In termination mode, the backend traffic (i.e. the traffic from the WAF to the web server) can be encrypted via SSL
All major cipher suites should be supported by the SSL v3 implementation.
Should support for hardware-based SSL acceleration or SSL off loading
High Availability and load balancing
Should support High Availability in active mode,
WAF appliance should have application-aware load-balancing engine to distribute traffic and route content across multiple web servers.
WAF appliance should support Data compression for better response time to users
Vulnerability Scanning.
The product must possess a Web Application Vulnerability Scanning capability-built in.
The vulnerability scan should identify vulnerabilities such as XSS, SQL injection, Source code disclosure, Common web server vulnerabilities etc..
Scan must be able to crawl the Web application
Must be able to scan the authenticated applications.
Should support scheduled scanning.
Should support exclusions in scanning by the administrator.
Authentication and Administrative access.
Should support Secure Administrative Access using HTTPS and SSH
Should support Role Based Access Control for Management
Ability to remotely manage boxes
Management User Interface support for both GUI and CLI access.
Separate network interface for SSH/HTTPS access.
Support for trusted hosts
Role-based management with user authentication.
Should support and two Factor Authentication
Logging and Reporting.
Ability to identify and notify system faults and loss of performance
Should support Log Aggregation
Should support multiple log formats such as CSV, Syslog, TXT, etc..
Should support inbuilt Reporting and sending the report via E-Mail
Should support report formats in PDF, HTML, WORD, RTF, etc..
Reports should be customizable.
Report Distribution Automatically via email
Should generate comprehensive event reports
Should be able to monitor real-time HTTP throughput

APT – Advance Persistent Threats

Anti-APT Specs
The solution should be able to communicate bi-directionally with the proposed UTM/NGFW, WAF, EMAIL Security solution for automatic blocking/threat update
The solution should support deep packet inspection of SSL encrypted traffic (including HTTPS) for both incoming and outgoing
The solution should provide detection, analysis and remediation capability against APT & SSL based APT attacks.

Anti-APT Specs
The solution must employ an on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats and must not be signature based.
Theproposedsolutionshouldbeabletodetectandpreventadvanced Malware,Zero-dayattack,spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signaturedatabase.
Theproposedsolutionshouldperformdynamicreal-timeanalysisofadvancedmalwaretoconfirmtrue zero-dayandtargetedattacks.Nofileshouldbesenttothirdpartysystemsorcloudinfrastructure system for analysis and detection of Malware
The proposed solution should automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware.
The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.
The proposed solution should analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications.
The solution must support pre-populated Licensed copies of Operating systems and applications/software's(likeMicrosoftOffice).Thereshouldbenorequirementforthecustomertobuy additional license.
The system should be able to support file sizes up to 200MB or more
The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, commonmultimediacontentssuchasJPEG/GIF/BMP/WMFandZIP/RAR/7ZIP/TNEFarchivesto prevent advanced Malware and Zero day attacks.
The proposed solution should capture, and store packet captures of traffic relevant to the analysis of detected threats.
The proposed solution should have the ability to display the geo-location of the remote command and control server(s) when possible.
The proposed solution should have the ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack.
The proposed solution should be able to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, SNMP, or HTTP POST).
The proposed solution should have the ability to be deployed in out-of-band mode (also SPAN/TAP) & inline mode
The proposed solution should be capable to block inbound malicious exploits delivered via a web channel and outbound call-back communications when deployed in inline, or out-of-band mode.
The proposed solution should support SMB / CIFS / NFS protocol for sharing and transferring files
Theproposedsolutionshouldprovidevisibilityintoscanhistoriesofeachfilescannedthatareaborted, completed, or inprogress.
The solution should provide reports in (but not limited to) PDF/CSV formats.
The solution should have anti-evasion capabilities to prevent malwares detection of being run/executed in the virtualized environment.
The solution should support for SIEM log integration.
The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc.
Minimum number of Interfaces - 4x GE and expandable
Number of VM's should be at least 14
It should support Sandbox Analysis for multiple operating systems like Windows 7, Windows 8.1, Windows 10 etc.

Anti-APT Specs
The APT appliance should be able to process minimum of 1000 files/hour or 500,000 files/month
High Availability & Maximum Scalability
The solution should have dual AC power supply fully populated (within box) from day one
APT, Firewall, Email Security must be from same OEM

Application Security

Minimum Technical Requirement
Solution must be capable of both Dynamic and static testing of applications
Solution may be from different OEM but must be capable of managing from same console
Solution must support all key languages for Static testing including SAP (ABAP)
Solution must support all key web application
Solution must support flexible deployment as required, like On-Premises or Over-cloud or Hybrid
Solution must have deployment in at least 5 government of India organization for last 2 years or more
ForDynamictestingsolutionmustbesizedfor2namesuserswithouthavinganylimitationonnumber of applications to bescanned
For Static testing solution must be sized for 10 applications (Code) without any limitations on number of time code to be tested.

Database Security

Minimum Technical Requirement
Encryption solution must be a platform to support Embedded Format preserving encryption to enable transparentkeyrotationandshouldseamlesslysupportcustombuiltapplicationsandcommerciallyoff the shelf software. It must be for 5Applications
Solution must be stateless supporting data masking, file level encryption, Data De-identification, Data Tokenization.
Solutionmustbecapableofformatpreservingencryptionofdataatsource(application)levelandmust be independent of any database which customer isusing.
It should work without schema changes in the databases where private data may reside and must integrate with proposed SIEM seamlessly.
It must comply to NIST-Standard FF1 AES Format-Preserving Encryption (SP800-38G) should be provided & necessary security proofs should be provided.
The encryption keys should be regenerated on the fly for future e-discovery and the data protected by the system may be shared without exchanging keys with an external party
If Solution is stateless then no key managers to be quoted else OEM Key managers in HA for DC and HA in DR must be quoted
Solution must take care of application level data as well as Database level
Solution must be licensed for at least 2 applications or higher to start with further scalable by adding application licenses

SOAR – (Security Orchestration, Automation, and Response)

Functional Requirements
Dashboard
Solution Should have a configurable Dashboard dependent on the role of the user

alerts reaching the SLA time period should be configured to show up in some manner
Dashboard should display alerts, Analyst Task
ROI should be configurable.
Alerts should be sorted by Severity
Each analyst must see his own workload
Dashboard should support import, Export
Dashboard should auto-refresh
Role wise dashboard view - T1, T2 or level 1, level 2 analysts
Solution must be able display mean time for identification, confirmation, containment, eradication, recovery, or aftermath for incident management
Solution must have dedicated dashboard to monitor health status / availability of each integration
Reporting
Report should be Customizable using UI
Report should allow Scheduling
admin should be able to export report to the below Format:
· PDF
· CVS
Report must be sent by Email
Access to reports be role dependent and controlled through RBAC
Solution must support recoding of audit logs for all the downloaded reports
Reports must have Metrics
Alerts Incidents/Case Management
Alerts and incidents should be handled separately
Alerts fields should be automatically changed to the relevant type of attack
Alerts should correlate with one another if they share the same type of attack, asset, or another applicable component
Audit trail (un-editable) should be available for each case
Interfaces must be customizable
Admin must be able to view raw logs from parsed/normalized data queries
Workflows/playbooks must establish what remediation actions an investigator can take and prevent actions that would unnecessarily make changes or cause evidence loss
User must be able to add new artifacts or IOCs upon investigation completion
User must be able to search for keywords across all fields of data
All updates, notes or actions must be able to be pushed from the investigation to a ticketing platform
Analystshouldhavetheabilitytorequestanewticketbecreatedintheticketingplatformwithrelevant informationincluded
Ticket must have the ability to automatic enrichment available for data like host, IP, file reputation, etc.
Admin must have the ability to Manage the comments (add, edit/delete/remove) or attachment (add, edit/delete/remove, search)
Ticket Metadata must offer various information on a selected ticket (who/when, ID, status, priority, queue)
Case management must support Role Based Access (RBAC)
Tickets escalation based on:
· Priority

· Risk
· Impact
· Age
Solution should be able of performing Root Cause Analysis (RCA – related to break-in cause)
Solution should be capable of performing Post Incident Analysis (PIA – related to incident handling)
Solution must have Customizable Playbooks/Workflows on how to handle an incident in different incidents (Email, web, endpoint infection)
Solution must support global search across all incidents for Notes & Description or other keywords in the incidents
Solution must support Incident Response Lifecycle (assignment/mapping/escalation)
Solution must support Mapping/Tagging tickets/ incident to Cyber Kill Chain phases
Solution must support SLA Tracking and alerting (Service Level Agreements of Incident Tracking)
Solution must manage the attachment as part of alert / incident management (add, edit/delete/remove, search)
Solution must provide detailed chain of custody for events viewed and data collected
Solution must support Threat Hunting / Track Campaigns
Solution must support search for the added IOCs in Log Management system
Solution must Provide the required logs related to specific IOCs in the tickets (Network logs/Endpoint Systems)
Playbooks
Solution must have at least 80 playbooks out of the box
reporting metrics of playbooks must be available (runtime, point of failure, etc.)
Playbook execution must create an audit trail in the case
Solution must have the ability to send update to the ticketing system from playbook steps and outcomes
Admin must have the ability to export Playbook
Solution must support running multiple playbooks at same time
Debugging tools must be available out of box with the tool
Solution must support creating playbooks with a visual interface
Playbook must support:

· manual actions and tasks
· Decision making
· Nested playbook concepts
· Python execution for custom scripts
· Rich text Emails
Tool must have at least 6 playbook initiation types
Analyst must have the ability a playbook and tag playbooks\Folders
Solution must have the ability to:
· data ingestion playbooks
· trigger reports from playbooks
· capture errors and failure reasons
· schedule playbooks
· have looping conditions and step
· add conditions to steps
· add mock output to steps
· ignore errors
· clone steps in and across playbooks
· align playbook steps automatically
· mark playbooks as private or public
Solution must control playbooks through RBAC
Solution must read PDF and data can be extracted to indicators
Solution must support playbook initiation on data update or delete
Solution must support versioning of the playbook
Solution must support export of single playbook / export linked playbook

Solution must support restarting the playbook from failed step
Connectors
vendor must provide consistent update and support to supplied connectors
vendor provide new connectors on future releases that are created by them
Vendor must provide documentation to setup integration with the supported connectors
Solution must have at least 250+ integration
Solution must send a notification about new update
Vendor must provide connector SDK without additional cost
Solution must have data ingestion wizard for SIEM, Exchange, TIP and related platforms
Solution must show integration/connector health status
IOCs Artifacts
Solution must have dedicated Indicators, Hunts and Complains module
IOCs must correlation across different incidents/tickets
Analyst can ingest bulk IOCs
Analyst can add, edit, delete, remove, search IOC
IOC can be grouped by Event, Campaign, Attacker, Vector, Sector Grouping
Analyst must be able to tag IOCs to the Cyber Kill Chain phases
Audit
Solution must record audit trail of all manual and automated steps, actions during execution of a playbook
Solution must be able to auto-document the entire incident workflow manual as well automated steps for all incidents timestamp of all actions taken in an incident.
Solution must monitor its usage to maintain a complete audit trail of system access, system modifications, any configuration are changed etc. Granular audit logs with details of “Who, What, When, where" with success/fail result for each and every activity of users.
User Management & RBAC
Solution must support role-based access control for segregation of alert/incident type to a role

Solution must support an easy menu for administrators/managers to add, modify, and delete users then provision access
Admin should be able to limit access to specific components (search, reports, run playbooks, etc.)
Solution must support Single sign on and two factor authentications
Deployment
Solution must have the ability to fully deployed on-prem
Solution must be provided on software OVA and deployed on Virtual infrastructure
Solution must easily transfer settings to an updated version
SOAR and SIEM must be from the same OEM only

SIEM - Security Information AndEvent Management

SIEM Specs
The SIEM solution should provide a dedicated appliance/Virtual Appliance solution with provision of scaling up with distributed architecture
The SIEM solution must be able to store both the raw event log as well as the parsed event log/normalized data.
There should be no requirement for a separate “storage” tier that filters or sends a subset of events forwarded by Collector / collectors to a correlation tier. The SIEM solution must be able to process every event forwarded by the collection tier.
The SIEM must be able to collect additional context beyond log data from devices and this should be achieved by actively discover the devices within the network without an agent and using standard protocols such as SNMP, WMI, VM SDK, JDBC, Telnet, SSH, JMX etc
Discovered device should be presented in a Configuration Management Database (CMDB) within the SIEM solution and display at a minimum Version/Firmware/OS installed on the device, Device serial number and Interfaces configured on the device with name, IP, subnet, status, interface speed, processes running on the device or operating system
Devices should automatically be populated within groups in the CMDB, for example Firewall Group and be able to report on all information within the CMDB including firmware of devices or version number, audit report with pass/fail whether the device has the appropriate version of Version/Firmware/OS installed on the device, collect performance metric of CPU, Memory, Disk . Process utilization etc
TheSIEMshouldprovideaunifiedanalyticsinterfacethatallowsthesamequerylanguagetoanalyse bothlogdataandperformancedata.Bothraw,parsedandenricheddatamustbepassedtotheSIEM solution from the collectors. Processing of event data should be performed by parsers on the system. All parsers should be able to be modified andcustomized.
Devices can be monitored without agents via SSH, telnet WMI, JMX and PowerShell.
Ability to integrate with Threat Intelligence (TI) feeds
Thesolutionshouldprovideoutoftheboxreports,atnoadditionalcharge,forPCI-DSS,HIPAA,SOX, NERC, FISMA, ISO, GLBA, GPG13, and SANS criticalcontrols

The solution should have the ability to export and import dashboards, reports and rules via XML. It should be able to collect network device configuration, identify changes and provide side-by-side comparisonandthedashboardvisualizationsmustsupportthefollowingcharttypesBar,Pie,Lineand Table
The SIEM solution should be customizable with virtualization support to manage overlapping systems and networks from a single dashboard

DDoS - Denial-of-Service Attack

DDoS Specifications
Architecture
The proposed solution should be appliance-based solution & Inspection and prevention must be done in hardware
Solution must be supplied with at least 8 x 1GE LAN & 8 x 1GE WAN interfaces and scalability to additional 2 LAN & 2 WAN interfaces
Solution must at least support 5 Gbps on Mix / production traffic
The device operating system should be hardened, and it should support high availability
Device management interface must be firewalled internally.
Performance should not be limited by any licensing system.
In inline mode system must not modify MAC or IP addresses of passed frames
Solution should support 1 Million simultaneous connections
Latency should be lower than 50 microseconds
The solution shall support IPV6 protocol.
The DDoS detection capability of the solution must not be impacted by asymmetric traffic routing.
The system must detect the attack dynamically without the need of any static control/redirection (E.g. route maps or static routes)
The system must have an updated threat feed that describes new malicious traffic (botnets, phishing, etc...).
The system should be capable to mitigate and detect both inbound and outbound traffic.
The DDoS detection solution shall have the learning mode to easily identify anomalies in the network communication.
Security
The system must be able to block invalid packets (including checks for Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped
ThesystemmustsupportthedroppingofidleTCPsessionsifclientdoesnotsendauser-configurable amount of data within a configurable initial timeperiod
The system must limit number of simultaneous TCP connections on a per-client basis
The system must allow protection parameters to be changed while a protection is running. Such change must not cause trafficinterruption
Solution should support security at layers 3,4 and 7
Solution should support for all 255 protocols at layer 3
Solution should support all 64k TCP and UDP ports
System must not use signatures; System must have methods of using behavioural and heuristic analysis
System must detect and block HTTP Opcode Flood
System must detect Excessive URL/source/second

System must be able to detect and block SYN Flood attacks
System must be able to detect and block Zombie Floods
System must be able to detect and block ICMP Floods
System must be able to detect and block Fragment Flood
System must be able to detect and block HTTP GET Flood
System must be able to detect and block Floods from Unwanted Geographical Areas
Deployment Options
Inline: - The DDoS appliance should support 'inline', meaning it is installed between the one or more protected systems and the rest of the network. In the simple network, data passes through the DDoS appliance as it travels to and from a protected system and the rest of an Ethernet local area network.
Protection Mechanism
DDoS Appliance should be completely Behavioural Based
It should measure byte and packet counts, state transitions, fragments, checksum, flags, new connections, address pairs, and so on as Layer 3 to Layer 7 parameters to define Threshold
In case of threshold violation traffic should be drop
It should be possible to write manual ACL's to block certain IP
It should be possible to block Geographical Locations to prevent flooding attacks from a country
IP Reputation
DDoS Appliance should receive a continuous update feed of Malicious Sources categorize as phishing, botnet etc.
When protection enabled traffic from these sources should be blocked

Central Core Switch

Specification Layer 3 Core Switch
The Core Switch Can be Chassis Based / Virtual Chassis based
Should have 48x 10/25G SFP28 with FC-FEC and RS-FEC support and 8x 40/100G QSFP28 ports.
Switch should be able to support copper Base-T (1G & 10G) over Cat6 media support and fibre 1G, 10G and 25G with Multi-mode and single-mode media support.
48x 25G SFP+ transceiver, 1x 100G 5Mtr DAC cable to be provided with Switch on day 1.
Transceivers should be from Same OEM of Switch.
Non-blocking architecture and Wire rate L2 & L3 forwarding. Throughput: 4000 Gbps and 1000 Mbps
Should have Redundant hot-swappable Fans & power supplies. Should have USB and console ports.
Should have x86 based multicore processor with minimum 8GB of RAM onboard
Switch should have modular operating system with ability to contain faults and repair/restart process state fully. Should have support for ISSU/fast-upgrade or live patching.
Should support 256K MAC address, 256K IPv4 prefix Routes, 4096 802.1Q VLANs
Should Support telnet, industry standard CLI, SSHv2, HTTPS, SCP, SFTP, NTP, DHCP server, PTP, SNMP v1/2/3, LLDP.
ShouldsupportAAA,TACACS+,Radius;MAC,IPandPortfiltersupportinACL;stormcontrol,Control plane protection fromDoS.
Should support QoS, COS/DSCP trust, 802.3x, PFC, ECN, priority Queuing, 8 queues per port, ACL based classification, 9200 bytes jumbo frame, policing and shaping.
Should have automation support with python, bash, API, ansible, dockers and zero touch provisioning for custom programmability and use cases.

Shouldhaveadvancemechanismsforin-depthtroubleshootingandmonitoringlikepacketcaptureon the device, port mirroring, targeted filtered mirroring, real-time streaming telemetry, microburst congestion detection and reporting, TWAMP,sFlow/Netflow.
ShouldsupportMSTP,perVLANRSTP,LACP,802.1qtrunking,Staticrouting,OSPFv2andOSPFv3, ISISv4andv6,RIP,PIM-SM,BGP,VRF,Anycast-RP,VRRPv4andv6,IGMP,BFD,64-wayECMP and PBR on day-1 with software ready support for advance protocols VXLAN+EVPN if required in future.
Should have NDCPP/EAL common criteria certification
HardwareandTACsupportshouldbedirectlyfromtheOEM.OEMshouldhave24x7TACsupported. For genuine parts replacement and proper maintenance of records for warranty, RMA should be processed directly by the OEM only. OEM email-id and India Contact support no. to beprovided.
Device should support same OS image as other devices in network for simplified operations and management.
Device should have Ipv6 ready with Ipv4 and Ipv6 dual stack support
0 to 40-degree Celsius operating temperature, 19" rack mountable with front to back airflow.
The Total solution should have 5 years hardware/Software/Licenses warranty for every item supplied as a part of solution. OEM of the proposed solution should be listed in Leaders Quadrant of Gartner's latest report in DC Networking

Access Switches

Performance and Scalability
Theswitchshouldhaveminimumof24*10/100/1GEthernetPortsand6*10/25GorbetterUplinkPorts in 1 RU fixed FormFactor
The switch should be at line rate, non -blocking architecture
Switch should have field replaceable power supplies and FAN trays
Switch should Provide persistent/constant PoE power even when switch is under maintenance
Each should be populated with 10/25G SR Multi Rate SFP from day one: Quantity 2
Shall support modern modular operating system designed for scalability and reliability
L2 Feature
Switch should support Ethernet standards like IEEE802.1p, IEEE802.1Q, Flow control, Jumbo frame, 802.1D, 802.1w, 802.1s, 802.3ad, private vlan
Switch should support vlan based on ports, MAC address, IP-Subnet based vlan / 802.1x, Minimum Throughput of 170 Gbps, System Memory 4GB, System Flash 4GB and Packet Buffer 6 MB. 64-way ECMP
Switch should support LLDP
Switch should support Ipv4 and Ipv6. The Switch should be able to discover (on both Ipv4 & Ipv6 Network) the neighbouring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.
Layer-3 Features
Switch must have routing protocols like BGPv4, OSPFv2/v3, ISISv4, BFD, PIM, SSM, Policy based routing
Switch should support VRRP, should support active-active port channelling mechanism.
Network security features
The switch should support IEEE 802.1x providing user authentication, authorization and CoA.
The switch should support SSHv2, SNMPv3, TACACS+ and RADIUS
The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network.

Switch should support Ingress ACL Scale of 4k or better.
Switch should support real time data collection with sFlow/Netflow.
Quality of Service (QoS) & Control
The switch should support 8 egress queues per port to enable differentiated management
The switch should support Standard 802.1p CoS field classification and Differentiated services code point (DSCP) field classification
The switch should support Rate Limiting function to guarantee bandwidth
Switch should support IEEE 1588/NTP
Operation and Management
SwitchshouldhavededicatedmanagementportandUSBportstouploadconfigurationfilesandimage
Management and Troubleshooting
Switch should support telnet, ssh, https, SNMPv3, configuration rollback feature for ease of management
Switch may support API Driven configuration and support Netconf and Restconf using YANG data model. It may support automation tool like python
Switch should support port mirroring based on Inbound & outbound, mirroring based on ports, vlans.
Switches need to be provided with all software license from day-1 as per RFP specification
Switch should support streaming telemetry
OEM of the proposed solution should be listed in Leaders Quadrant of Gartner's latest report in DC Networking

SMARTRACK for Datacenter (Integrated & Built-in Devices Space, Precision AC, Fire Suppression, UPS and related accessories)

Description of Requirements
This specification covers intelligent integrated/inbuilt infrastructure, standalone system design, engineering, manufacture, assembly, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed Data Centre to be installed, as detailed in the specification, complete with all accessories required for efficient and trouble free operations
Modular and scalable design for power and cooling: All the components used to design the system should be redundant and in the Events of failure the components can be maintained easily. All the components of the infrastructure should be such that it can be easily dismantled and Relocated to different location.
Requirements
Intelligent Integrated Infrastructure with inbuilt hot and cold aisle containment of 2 racks should cater IT load up to 10KW.
Intelligent Integrated Infrastructure essentially should include internal redundant or backup power supplies, environmental controls (Precision air conditioning, fire suppression, smoke detection, Water leak detection and humidity sensors), and security devices. Critical systems like UPS and Precision Air-conditioning systems should have N+N topology. Environmental monitoring shall be done from IP based software.
The detail specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be in adherence to standard Data Centre guidelines thus shall be composed of multiple active power and cooling distribution paths, but only one path active. Shall have redundant components.
The Intelligent integrated Infrastructure shall have following components: -

In-Row closed loop Air-Conditioning
Data centre server and network racks should be equipped with In-row Variable / digital scroll cooling units to provide closed loop precision cooling system which should be able to cool the equipment's uniformly right from 1stU to 42ndU of Rack
Each Precision Air Cooling should be of min 10kW capacity N+N topology. Precision Air Conditioner should have following Features: Cooling System should be DX (Variable) type in N+1 Topology Inbuilt Heater and Humidifier to cater IT load up to 10kVA Outdoor Unit
Power Distribution
Intelligent Rack PDU (Vertical) – with 30 sockets (24 nos of IEC C13 Sockets & 4 nos of IEC C19 Socket with 2.5 mtr power chord with 32A MCB)-02 Nos. for each Rack (each rack is having two PDU's).
Main Electrical Panel and Cabling
DB panel should be mounted on to utility rack/room wall with all internal cabling integrated into the same. Essential MCB/MCCB should be provided with electrical system. All the PDUs inside all racks should be connected by the UPS. DBpanelmountedonUtilityrackshallbecoveredwithNovec1230Gasbasedfiresuppressionsystem
Fire Detection and Suppression
Fire detection and suppression system: Fire detection and suppression system should be mounted in paneladjacenttoSmartRackstoavoidconsumptionofanyusableUspaceanIn-rackbuilt-infeature of solution. It should have Fire alarm and fire suppression unit and the fire suppression agentshould be NOVEC 1230 Gas as per NFPA 2001 guidelines
Blanking Panel: 70%
Environmental Controls
Each set of intelligent rack should include basic environmental controls: Smoke Detector Water Leak Detection system Temperature/ Humidity Sensor Door Sensor Alarm beacon
VESDA for the Integrated Server Racks for early detection of the fire incident.
U Space
Intelligent racks should have Min 240 U (total) space available for IT equipment's and network equipment.
Racks
42 U racks of dimension 600 mm x 1000 mm - 5 numbers 42 U racks of dimension 800 mm x 1000 mm - 1 numbers
These rack enclosures should have both integrated cold aisle & hot aisle containment of minimum 300mm each for proper airflow
Monitoring
Each set of Integrated racks should have IP based monitoring facility of all the passive parameters inside racks.
Capable for Email Alerts
Monitoring unit should not occupy more than 1U space
Other features:
The Intelligent integrated infrastructure would provide much functionality and some of the key functionalities are – Both Cold aisle & hot aisle containment should be of minimum 300mm each for airflow, Airtight Thermally insulated cabinet, remote management.
Intelligent integrated infrastructure would have provision to add an extra rack in future. It should be flexible, adaptable, controllable infrastructure.
Rack based Biometric access control system provided should be controlled by access control panel with access control for both front as well as rear doors. IP based Access control with user exclusive authentication
Critical Component's for Integrated Server Racks system (Rack, rack PDU, Cooling, UPS and

monitoring system) should be from same & single OEM for Seamless Integration & better Service Supports
Air-conditioning Condenser unit designed for higher efficiency ikW/Tr of 0.1 or less
IP based Access control with user exclusive authentication
Monitoring SNMP Enablement feature to connect to any 3rd party BMS over SNMP
HMI – Graphical User Interface for Smart Racks monitoring
Electrical Distribution board within Utility Cabinet to have fire detection &Novec Based Fire Suppression system
Dual Electrical Panels for Distributed power architecture to avoid single point of failure
Status based LED Lights
Precision Air Conditioning System of 10kW Capacity (N+N)
Configuration
Supply, installation, testing and commissioning of DX Type Air-conditioning units designed specifically for high sensible heat ratio with variable cooling technique to match the low latent loads of systems to be installed in the integrated cabinet for effective and uniform distribution of cooling.
Direct Expansion
Cooling Circuits–One refrigeration circuit, incorporating a high efficiency, fully hermetic variable capacity compressor with crankcase heater, safety valve, filter drier, moisture indicating sight glass, liquid line solenoid valve and an externally equalized expansion valve.
- Each compressor is equipped with pre-set high- and low-pressure switches for protection against high condensing and low evaporating temperatures. The low-pressure switch features an automatic reset (with an adjustable delay for winter start-up). - The unit shall be provided with additional protection against high ambient temperature. When the temperature goes over the design conditions, the unit remains in operation with partial load (20% decrease against required). If such protection is not sufficient High-Pressure switch shall generate a high-pressure alarm and the unit shuts down – manual reset shall be required. - The inclined evaporator coil is manufactured from copper tubes, mechanically bonded to hydrophilic painted aluminum fins, with a stainless-steel condensate drain pan. The large face area/low velocity coil allows precise control of temperature and humidity* during cooling and dehumidification* and is designed to optimize fluid velocity and minimize pressure drop. - The moisture indicating sight glass, liquid line solenoid valve and expansion valve for each circuit are mounted in a service compartment, isolated from the air stream, to allow checking and adjustment while the unit is in operation.
Fan Section - Units is offered with two plug EC Direct Drive Fan, High efficiency, external rotor electronically commutated (EC) motor with integrated electronics, True soft start characteristics (inrush current lower than operating current), Backward curve, corrosion resistant aluminum fan wheel, Maintenance free design and construction. The fan section shall be designed for higher air flow. The fan shall be protected over temperature of motor, electronics, locked rotor protection, short circuit of motor output. Fans are IP54, Protection class F.
Cabinet and Frame - The unit shall be powder painted panels with ½" (or 10mm) insulation. A hinged control access panel opens to a second front panel which is a protection enclosure for high voltage components. The frame is painted with a powder coat finish to protect against corrosion. The unit is totally front and rear accessible including any component removal.
Air Filtration - The filter cells are made of two deep pleated 4" filters rated MERV8 following ASHRAE 52.2 (45% by ASHRAE 52.1) or G4 following EN779, located within the cabinet, and accessible from the rear of the unit. Frame of the filter shall be made of galvanized steel. - Clogged filter alarm is available for standard and for optional filter. It sends a visual alarm to display.
Refrigerant All units equipped with direct expansion circuit are suitable for R410A refrigerant.
Microprocessor Controller - Air conditioning models should be controlled by microprocessor-based controller. It can be

programmed to control the function of every device within the unit via I/O.

- The controller allows setting and monitoring of the room parameters. Unit utilizes multiple temperature sensors placed at the rack inlet, to ensure management and control of temperature by rack. Each unit should be connected up to 10 Sensors.

The controller should allow setting and monitoring of the following space parameters:

- Air inlet Temperature
- Air supply Temperature (remote sensors at rack inlet)
- Return Temperature set-point
- Supply Temperature set-point
- Return Temperature band
- Supply Temperature band
- Humidity (inlet)
- Humidity set-point
- Humidity band
- Rack Min, Max and Average temperature The

example of available warnings / alarms:

- High supply temperature
- Low supply temperature
- High return humidity
- Low return humidity
- Loss of airflow
- Compressor Low Pressure
- Compressor High Pressure
- Electrical heater high temperature (When applicable)
- Clogged filter
- Customer input (No 4 inputs)
- LP transducer fail
- Call service (customer input)
- High temperature (customer input)
- Unit hours exceeded
- Compressor hours exceed
- Humidifier hours exceed
- Supply sensor failure
- Network failure
- Humidifier problem
- Digital scroll high temperature
- Smoke detected
- Fire alarm
- Rack sensor failure, etc.

Following features should be incorporated in the controller:

- Status Report of the latest 400 event-messages of the unit.
- Input for remote on-off and volt-free contacts for simple remote monitoring of low and high priority alarms: high/low temperature, high/low refrigerant pressure, fan/control failure, compressor/control failure and others are available
- LAN management: functions provided as standard include stand-by (in case of failure of the unit in operation, the second one starts automatically), and automatic rotation. At least one unit in the LAN has to be equipped with Cold Fire large display
- Automatic restart is provided after a power failure.

Monitoring

- There should be SNMP and HTTP/Web-management capability for enhanced communications and control of HPM systems. The cards make use of an Ethernet network (10/100Mbit) to monitor and control a wide range of operating parameters, alarms and notifications thanks to a standard web browser (Internet Explorer). The card utilizes standard Ethernet cables (different cable lengths

are available for your convenience on the Connectivity price list). - The unit shall also include input volt-free contacts for simple remote monitoring of low and high priority alarms: high/low temperature, high/low refrigerant pressure, fan/control failure, compressor/control failure and others are available.
Condenser
- The condenser should be with fan speed controller designed & set for usages of R410A refrigerant. Condenser should be worked -20 deg C to 46 deg C ambient temperature. The condenser frame shall be made up of a sturdy GI structure. The motorized fan shall be IP54, protection class F
Humidifier - The unit is fitted with a canister type steam humidifier suitable for use with water of varying degrees of hardness, provided that the water is not treated or demineralized (Conductivity range 125-500¤S/cm). The humidifier is complete with a water inlet valve, water outlet valve and a maximum water level sensor, disposable cylinder, steam distributor and electronic controls. Humidifier control is of the ON-OFF type, can be also disabled by remote contact (Optional – humidifier and reheat lockout). Humidifier is removable from the rear of the cabinet.
Racks & Accessories
Rack Containment Frame is 42 U, 19'' mounting type with standard Rack + Cold & Hot Aisle Containment
Rack frame is, scalable and modular with safe load carrying capacity of 1000 Kg
Colour shade of Rack is RAL 7021/9005 (Black)
Base plinth with 100 mm height
Cable entry provision from top & bottom both side of rack
Cut outs with rubber grommet on top and bottom cover of rack for cable entry
Vertical Cable manager on both LHS & RHS on rear side
Front glass door for complete 42U height visibility & rear split steel door
Thermally insulated cold aisle chamber
Blanking panels to prevent air mixing
Fixed Shelf to be provided
Plastic Cable duct on vertical LH & RH section of racks for cable routing
Front Rack doors to be provided with Biometric Access Control with 02 nos. of Electromagnetic lock per door
Gas spring to be provided on front doors of racks
Status based LED light to be provided on each rack
Safety and Security Systems
Biometric Based Access Control - The IP based Access Control System shall be used to serve the objective of allowing access to authorized personnel only. The system deployed will be based on Biometric Technology. The front & rear rack doors will be provided with magnetic locks and will operate on fail-safe principle through one common Biometric access control system. The system would be designed and implemented to provide following functionality: - Configurable system for user defined access - Built-in Real Time Clock (RTC), calendar; complete Database stored locally and shall be capable of operating offline on standalone mode - Record, report and archive each and every activity (permission granted and / or rejected) with log formats - Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc. - At the biometric reader, user presents the finger to the biometric reader which is unique to each employee. The pattern is read and compared with stored data to grant / deny access.
Fire Alarm and Fire Suppression System - The integrated infrastructure solution should be designed as a complete stand-alone unit with security, fire detection and fire suppression systems. Each of the systems is inter-operable and inter-connected.
Environmentally friendly NOVEC 1230 agent is used to ensure that no harm to human beings and environment is caused. Following systems should be installed.

- NOVEC 1230 Clean Agent for fire suppression system - Fire detection and alarm systems, with detectors and panel. - Access control system. - Protected area: The entire enclosed volume of the Intelligent Rack containment is protected with fire detection and fire suppression system. The doors are secured by Access Control system. - The NOVEC 1230 system is designed and installed as per NFPA 2001-2012 Edition. SMPV, Petroleum and Safety Explosives Organization (PESO) approved cylinder filled with NOVEC 1230 is installed in specially designed Modular rack. - VESDA system for the Integrated Server Racks.
Monitoring
- Supply and installation of 1U rack mountable monitoring system with Sensors & notification system. The system shall continuously collect critical information from network connected devices such as UPS system, Cooling Units, temperature & humidity sensors, Door sensors, Water Leak sensor and other dry contact monitoring. Beacon & Buzzer-Sound and Flash Led Alarm. Based on pre-set parameters, automated email alerts are sent to the intended recipients
Intelligent Rack environment remote monitoring
Modbus 485 Communications
SNMP Communication
Single window for monitoring all sensors
Data and logs of historical information of alarms and notification
Temperature & Humidity Sensor, with LCD display and RJ45 connector
Door opening sensor with RJ 45 connector
Water leak detection sensor with RJ45 connector
Smoke detection sensor with RJ45 connector
Alarm device with LED flash and sound option
HMI – Smart Racks Graphical Interface
- Smart Racks should have functionality to graphically monitor the passive infrastructure ---- - 9-inch wide touch screen HMI display with a very user-friendly interface - It should be menu driven system, Thermal management, Power supply environmental quantities, alarms, logs, and provided a total of menu items, breakdown of the sub-menu item the next menu level, - First authorization on LCD, is only authorized once, authorized system will automatically skip the authorization page while booting - System Configuration page includes integrated cabinet configuration - Home page presents system function information (Such as Date & Time ex.), system performance parameters and critical system parameters
System performance parameters:
- Enclosures: thermal path average temperature, the IT load cabinet single cabinet (configured for an intelligent PDU). - Air conditioning: return air temperature, supply air temperature - All the components (Intelligent PDUs ext.) shall be graphically represented on HMI - Real time PUE should be displayed on the screen.
Critical system parameters: - UPS operation: AC mode/bypass mode/Battery mode/standby mode, The system load factor - HVAC Operation – Animated fan during Run & Compressor status display - IT racks parameters – Temp. & Humidity Parameters are highlighted for normal & abnormal values
Thermal Management: - Return air temperature profile cross-ordinate - cooling fan state to the operating state, the corresponding icon is animated; alarm flood state is, icon animation - Door status icon static display, the door opened and closed the door to a different style static icon.

Supply & Distribution:

- UPS page displays for the distribution parameters and real-time power system operating mode
- UPS working state: AC mode / bypass mode / Battery mode / standby mode
- The operating state of the system: Single / 1 + 1 parallel / 2N double bus
- For each PDU distribution -PDU page displays the total current and power component
- when the PDU voltage value, the current value exceeds the set range, the system will generate a corresponding alarm; on the contrary, the alarm disappears

Environmental Amount: (The amount of ambient acquisition)

- acquisition and display status of the current environmental data amount of the rack, comprising: a real-time value of the respective collection point temperature and humidity sensors, front and rear door state, hot/cold aisles average temperature curve moisture profile
- When the air conditioning is working properly, hot and cold airflow patterns dynamic channel is turned on when the air conditioning is not working, dynamic airflow patterns hot and cold aisles disappear
- Door status icon static display, the door opened and closed the door to a different style static icon
- when the passage of hot / cold temperature and humidity sensor measured value exceeds the set range, the system will generate a corresponding alarm; conversely, when the hot / cold aisles temperature and humidity sensor measurement range is set to fall the alarm disappears

Warning – Alarm-Current Alarm:

- Displays the Current Alarms Page
- The current alarm is divided into emergency alarms, major alarms and general alarms
- When the current alarms and buzzers system in the normal mode, the LCD buzzer will sound an alarm, and for 5 minutes, the duration of the latest alarm generation time from a timer
- In maintenance mode, the buzzer will not sound an alarm. After the lifting of maintenance mode, buzzer return to normal mode

Alarm – historical alarm:

- Alarm History page provides a display system and screening history alarms
- LCD page provides only historical records up to 100 within the system one week. For longer or more the number of alarm history, Web pages can be viewed in alarm management

Cleaning

- On completion of installation, testing of the system all components, cabinets etc. shall be cleaned & unwanted material, debris shall be removed from site. Scratches dents if any shall be cleaned & touched up to match the original finish Cable and electric wire should be

arranged in a way that minimize the physical tempering with the existing infrastructure and should be properly managed maintaining the aesthetics

Uninterrupted Power Supply (UPS) System

General Description:

Supply, install, test and commissioning of true online, double conversion, high efficiency, and high- power factor Uninterruptible Power Systems (UPS) rated at 2 x 40 kVA with combined battery backup support for 30 minutes on full load. UPS should be Rack Mountable & the backup batteries should be supplied with the necessary arrangements to mount outside the cabinet.

Configuration: 2 x 10kVA (N+N Redundancy)

Scope

- The scope shall include design, supply, installation, testing and commissioning of the complete UPS system and related accessories including:
- All Server racks will get power feed from two independent 40kVA UPS systems to ensure redundancy.
- All systems should be tested in factory as per the manufactures recommended procedure for all operating parameters and the test results should be provided during the installation.
- Delivery at site, unloading, handling, installation of complete system including interconnection from the UPS system to batteries and to input / output panels switches. All interconnections shall be done using multi-strand Flexible Copper conductor cables of appropriate sizes.
- Scope includes battery bank connections and providing safety barriers for all bus bars and cable connection leads on battery racks.

- Energizing of UPS and Battery bank commissioning.
- UPS control parameters setting and complete testing of system on load.
- Service backup by engineer till system is fully operational and subsequently training is to be provided to the concerned persons of the Institute.
- Any upgrade of the system hardware and associated other software during the warranty period should be supplied at free of charge.
- Acceptance tests will be carried out after installation and the systems will be taken over only after successful completion of the acceptance tests. –
- Operation and service manuals of the systems containing technical / Electronic drawings / circuit diagrams complete in all respects should be supplied. -

Specification / features of the Each UPS system are as follows:

- Widest input range.
- Double conversion and IGBT technology.
- Full IGBT Rectifier / Battery charger
- IGBT based Inverter
- Batteries to support 30minutes backup on full load
- Power distribution panels
- Facility for remote viewing
- Easy to expand in a cost-effective way

UPS other technical specification

General	
UPS type	ON-LINE
Model Name	Vendor to specify
Rating (VA/W)	Vendor to specify
Make	Vendor to specify
Technology	IGBT with PWM Switching
Crest Factor	3:1
Invert efficiency	>96 %
Overall efficiency	94.5 %
INPUT RATINGS	
Nominal Input Voltage	415V AC (3-Phase)
Permissible input voltage variation at full load	228 V – 478 VAC
Nominal input frequency	50 Hz
Permissible input frequencies variation	40 Hz to 70 Hz
Input power factor at full load	> 0.99 at full load
Input socket	Anderson connectors
OUT PUT RATINGS	
Nominal output voltage	380V (3-phase) / 230V (1-phase)
Output Voltage regulation	< +/- 1%
Output voltage distortion	<2% total harmonic distortion (THD) for 100% linear loads <5% THD for 100% non-linear loads.
Nominal output frequency	50 Hz
Waveform	Pure Sine wave
Power factor	0.9 lagging
Overload capability	125% for 5 minutes, 150% of full load for 1 minute, with automatic transfer to bypass
Output sockets	Anderson connectors
Transient recovery time	Within 20 milliseconds to +/- 1%
BYPASS	
Voltage Range	+15% -20%
Frequency	50/ 60Hz

Frequency Range	+/-20%
BATTERY PARAMETERS	
Type	SMF
No. of battery blocks	32-40
Battery nominal voltage	12V
Battery Voltage	384-480Vdc
ENVIRONMENTAL PARAMETERS	
Operating temperature	0 to 45 deg. Centigrade
Storage temperature	-15 to 45 deg. Centigrade
Relative Humidity	95% RH noncondensing
Altitude	1000 meters
Temperature de-rating	30-40deg de-rating
Altitude de-rating	< 1000m; derating according to GB/T3859.2 when higher than 1000m
Noise level	<58db
MECHANICAL PARAMETERS	
Height X width X Depth (MM)	Vendor to specify
Weight	Vendor to specify
Ventilation	Forced – Air cooled
Cable Entry	terminal block
Colour / Panel finish	EG7021
Protection	IP20
MONITORING SOFTWARE	SNMP, Dry contact card, site monitoring

Minimum Qualification for Smart Rack OEM:

A. Critical Component's for Integrated Server Racks system (Rack, rack PDU, Cooling, UPS,and monitoring system) should be from same & single OEM for Seamless Integration & better ServiceSupports
B. The OEM should have at least 3 years of experience in executing similar works (Similar works means – "Setting up of Modular & Integrated Data Centre infrastructure") in Central/State/PSUOrganizations.
C. The OEM must have executed minimum 5 Integrated Data Centre projects during the last 5 years from the of bid submissiondate.
D. OEM Service Support for Major Equipment: OEM or Manufacturer should have its own local service center in the state of Assam / Northeast/ WestBengal.
E. The OEM should have at least three qualified and experienced DC certified professionalslikeCDCP/CDCS/CDCE/ATDontheircompanypayrollwithminimum3years'experiencein Data Centre designing andimplementation
F. OEM shall be present in Gartner Competitive Landscape Research Report for Edge in the Micro Modular Data Centre Market as Leader in Data Centre FacilitiesSpecialist.

SDWAN – Branch / Site Office

SDWAN at Branch / Site Office Level
Firewall
The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operatingsystemthateliminatesthesecurityrisksassociatedwithgeneral-purposeoperatingsystemsand should have dual internal power supply from dayone.
The Proposed Firewall Vendor should be in the Leader's Quadrant of Gartner for NGFW.

SDWAN at Branch / Site Office Level
Firewall appliance should have at least 10 x 1GE interfaces, 4 x 1GbE SFP interfaces and 2x 10G SFP+ slot
Firewall Throughput should be 20 Gbps
Firewall should support minimum 10 Gbps of VPN throughput
Firewall should support 2000 site-to-site & client to site VPN Tunnels.
Firewall should support minimum 200 concurrent SSL VPN users and should be scalable in future
Firewall should support 50,000 new sessions per second
Firewall should support 1.5 Million concurrent sessions
The solution should support minimum 1.5 Gbps of NGFW (FW + IPS + AVC) throughput for Mix / production traffic
The solution should support minimum 1 Gbps of Threat Prevention (FW + IPS + AVC + AV/Malware) throughput for Mix / production traffic
The Firewall solution should support NAT64, NAT46, DNS64 & DHCPv6
The proposed system should have integrated Traffic Shaping functionality.
The Firewall should have SDWAN feature to support minimum 4 service provider for load balancing at same time in active/active.
Solution should provide transport independence and should allow to use any transport like MPLS, Internet, 3G/4G, Point to Point link
Management and SDWAN solution should communicate over encrypted channel
The Firewall & IPSEC VPN module shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification.
The proposed system should support
signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
b) PPTP VPN
c) L2TP VPN
The device shall utilize inbuilt hardware VPN acceleration:
a) IPSEC (DES, 3DES, AES) encryption/decryption
b) SSL encryption/decryption
The system shall support the following IPSEC VPN capabilities:
a) Multi-zone VPN supports.
b) IPSec, ESP security.

SDWAN at Branch / Site Office Level
c) Supports NAT traversal
d) Supports Hub and Spoke architecture
e) Supports Redundant gateway architecture
The system shall support 2 forms of site-to-site VPN configurations:
a) Route based IPSec tunnel
b) Policy based IPSec tunnel
The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode.
The system shall provide Ipv6 IPSec feature to support for secure Ipv6 traffic in an IPSec VPN.
Virtualization
The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 5 Virtual Firewall license should be provided.
Intrusion Prevention System
The IPS capability shall minimally attain NSS Certification
IPS throughput should be minimum 2.5 Gbps for Mix / Production traffic
The IPS detection methodologies shall consist of:
a) Signature based detection using real time updated database
b) Anomaly based detection that is based on thresholds
The IPS system shall have at least 7,000 signatures
IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available
In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked, and the Firewall will continue to operate while the problem is resolved
IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy lookups.

SDWAN at Branch / Site Office Level
IPS signatures should have a configurable action like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident
Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
Antivirus /Antimalware
Firewall should have integrated Antivirus solution if not please quote separate appliance
The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services:
a) HTTP, HTTPS
b) SMTP, SMTPS
c) POP3, POP3S
d) IMAP, IMAPS
e) FTP, FTPS
The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, unknow malware and targeted Advanced Persistent Threat without relying on just Signature database.
The proposed solution should be able to perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero- day and targeted attacks. Cloud infrastructure system for analysis and detection of Malware.
The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
Web Content Filtering
The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.
The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
The proposed system shall provide web content filtering features:
a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.
b) Shall include Web URL block
c) Shall include score-based web keyword block
d) Shall include Web Exempt List

SDWAN at Branch / Site Office Level
The proposed system shall be able to queries a real time database of over 110 million + rated websites categorized into 70+ unique content categories.
Application Control
The proposed system shall have the ability to detect, log and take action against network traffic based on over 2000 application signatures
The application signatures shall be manual or automatically updated
The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions
Data Leakage Prevention
The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.
High Availability
The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component
The device shall support stateful session maintenance in the event of a fail-over to a standby unit.
High Availability Configurations should support Active/Active or Active/ Passive
The SDWAN Branch / ZO device must be same as the Controller device at HO

UPS at Site Office Level

Technology
- IGBT based PWM Technology (b)Microprocessor controlled Digital Design (c)Double Conversion True On-line UPS (d) Manufacturer: IS9001 and IS14001 Certified and Small 2U height maximizes available space. Rackmount with user replaceable battery and Add on batteries for extended back-ups
Overall Efficiency (AC-AC)
> 90 percentage
Input Voltage and Range
230V 50Hz and Range 160- 280V (Full Load) and 230V 50Hz and Range 100- 280V (Half Load)
Input Frequency Range
50-60Hz
Input Phase
Single Phase with ground
Input Power Factor
0.95 or better
Output Voltage
220VAC-230VAC
Voltage Regulation

+/- 3percentage
Frequency
50 Hz +/- 0.1percentage
Harmonic Distortion (THD)
< 3percentage (linear load)
Output Waveform
Pure Sine wave
Crest Factor
3 ratio 01
Output Power Factor
0.8 or more
Battery Backup
Min 1-hour battery backup
Battery Type
Sealed Lead Maintenance Free VRLA type (Lead Calcium SMF batteries NOT acceptable)
DC Bus Voltage
As per OEM Architecture
Transfer Time
0 ms
Battery Enclosure
MS Rack Powder Coated
Operating Temperature
0 to 40 Degree C
Noise Level
<55 dB @ 1 Meter
Alarms and Indications
All necessary alarms and indications essential for performance monitoring of UPS to be incorporated.
Bypass
Automatic Bypass Switch
Compatibility
UPS must be compatible with DG Set supply
Communication Interface
(a)Standard RS 232 port for software interface (b)Standard SNMP interface support
Dimension(H*W*D)
Must declare
Certifications
IS9001 and IS14000 and EN 60950 and EN/IEC 62040-2 and cULus and CE and Federal Communications Commission
Environmental Compliance
RoHS 7b Exemption
The UPS at HO & ZO/Branch should be from the same OEM only

Passive Components

Cat 6 UTP Cable
4 Pair Cable with integral cross -member pair separator for uniform characteristic impedance.

Category 6 Unshielded Twisted 4 Pair 100 Ω cable shall be compliant with ANSI/TIA/EIA-568-D-2018 Additional ISO/IEC 11801-1 and ISO/IEC 61156-5 Transmission Performance Specification for 4 Pair 100Ω an guaranteed up to 1G Category 6 Cabling
Category 6 UTP cables shall extend between the work area location and its associated telecommunications closet and consist of 4 pair, UTP CM cable jacket.
Conductor: Solid Copper
Conductor Diameter: 0.555+-0.01mm (23AWG)
Insulator HD Polyethylene solid
Jacket: LSZH RoHS IEC 60332-3-22 complied, Colour- Grey/Blue
Outer Diameter: 6.0 ± 0.2mm
Max Temperature: -20°C to +70°C
Should be ETL certified and 4 Channel ETL Verified as per TIA 568-D-2018
Mechanical Test
Should have Pulling force of 11.5Kg.
Bend Radius: Installation: <4 X Cable Diameter at–20°C±1°C, Operation: <4 X Cable Diameter at –20°C ±1°C
Electrical Test
ConductorResistance: <9.38Ω/100m
ResistanceUnbalance 5%Max
MutualCapacitance: < 5.6nF/100m
Capacitance Unbalance:330pF/100m.
Propagation Velocity: 69%
ELT certified for 4 Channel should be submitted along with bid submission
Cat 6 UTP RJ 45 Keystone Jack
RJ45JackofCategory6,fortheestablishingoftransmissionchannelsofclassEwithupto4plugged connections, complies with Category 6 requirements of the standards ISO/IEC 11801-1, EN 50173-1, DIN EN 50173-1: 2002 as well as ANSI/TIA/EIA 568-D, de-embedded tested in acc. With IEC 60603- 7 (603-7), interoperable and backwards compatible with Cat.5e andCat.5.
Suitable for 10Gbase-T applications in acc. With IEEE 802.3an up to 500 MHz and 55 m.
CompatiblewithRJstandardplugs(RJ11,RJ12,RJ45),PCB-andtool-basedconnectionofinstallation cables AWG 24 – 22 (0.5 mm – 0.65 mm) and flexible cables AWG 26/7 – AWG22/7.
IDCterminationshouldfeaturenilcrossoverinacc.WithEIA/TIA568-A/B,gold-platedbronzecontacts formatingcycleupto750andinsertionForce20N;Retentionstrength7.7KgbetweenJackandplug
Material: RoHS complied
Housing material: Polycarbonate (UL-94-V0)
Should be available with dust protection feature
Should be 3P Delta certified for 4PPOE; ETL 4 channel Verified Certificate to be submitted along with Bid submission
19" 1U 24 port unshielded Straight Patch Panel
Patch panel should be modular design, models accommodate up to 24 UTP keystone-type jacks in 1U
RJ45 Jack of Category 6, for the establishing of transmission channels of class E with up to 4 plugged connections, complies with Category 6 requirements of the standards ISO/IEC 11801-1, EN 50173-1, DIN EN 50173-1: 2002 as well as ANSI/TIA/EIA 568-D, de-embedded tested in acc. With IEC 60603- 7 (603-7), interoperable and backwards compatible with Cat.5e and Cat.5.

Patch panel should be Enhanced cable strain relief is provided by a cable retention tray
Material: sub-rack made of Aluminum with dimension 44.4 mm: 482.6 mm: 105 mm (h:w:d) tray
Information Outlet or connecting module should comply with the specification mentioned above in 1.2
Standard: Conforms to IEC-60603-7 (603-7) for keystone-type, Snap-on apertures
Should be RoHS complied
Patch Cord, U/UTP 4P, Cat.6, length 1Mts, 2Mts, 3-5Mts
Standardization: Compliant with Cat.6, Class E requirements: ISO/IEC 11801 2nd Edition Compliant with Cat.6 component standards IEC 60603-7-4 and 60603-7-5
Tested up to 600 MHz
Cable shield: U/UTP
Number of conductors: 8
Stranding: 7 x 0.20 mm (24 AWG)
Cable jacket characteristics: cable, metal-free – LSZH RoHS complied
Cable overall diameter: 6.5±0.2 mm
Tube / Wire type: stranded conductor
Insulation: solid polyolefin, 0.97±0.02 mm diameter
Plug: Feature cable retention, with enhanced pull strength.
Cat 6 patch cord plug to have round cable holder and strain relief boot to avoid bending.
Plug should have high repeatability cross talk performance
Should be ETL verified for 4 channel and certified; RoHS complied
Faceplate
Should be UK style Keystone-type Faceplates are available in 1, 2 & 4 port configurations
Should be featured with shutter options
Should support Work with both Flush and Wall mount box
Should support Operating Temperature: -10～+60; Storage Temperature: -40～+68; Humidity: 10%~90% RH
Material: ABS, UL 94V-0; Spring: SUS304; Surface Finish: Polished
Fibre Optic LIU Rack Mount LIU (12-Ports)
Should supports up to 12 duplex SC adapters (24 fibres)
Pull-out drawer enables ease of access to the fibre
Height: 1 U, 1.75 inches rack mounting brackets allow for recessed panel mounting, enhancing cable protection
Rear cable entry cut-outs including one cable entry gland
There should be moving tray that provides built-in cable management by holding and arranging the cables
H: 44 mm / 1.72” (1U); W: 483 mm / 19”; D: 200 mm / 8” (face to rear); Weight:2.6 kg
Materials: Steel: Colour: Black with white silk-screened markings
12/24 Port SC Type Adaptor & Plates (Single mode)
High performance single mode and multi-mode connectors and adapters
Push-pull coupling for easy insertion and high repeatability
High system durability, stability and repeatability
Precision adapters with rugged phosphor-bronze alignment sleeves
PC and precision APC ferrules for single mode applications
PC ferrules: Insertion Loss < 0.3 dB typical; Return Loss > 26 dB typical
Should be designed to NTT-SC standards
Design, should provide non-optical disconnect terminations in a push-pull coupling mechanism, has been

tested to the rigorous Bellcore 326 standards
Temperature range: storage &operating -40°C to +80°C
Patch Cord, LC to LC, SC LC, Duplex, SM, G657A2, bend in sensitive PC, LSZH
Cable: SC-LC 9/125µm OS2 Single mode Duplex Patch Cord Length: 3mtrs
Connectors: The optical fibre patch leads shall comprise of Single mode 9/125µm fibre with 2XLC type fibre connectors terminated at one end of fibre patch cord and 2xSC type connector at other end of the fibre patch cord
Insertion loss should be better than 0.35 dB
Jacket Material: LSZH complying to IEC 61034-1 & 2, IEC-60332-1, IEC-60754-1 & 2
Attenuation: 1310/1550: 0.36/0.22 dB/KM
Connector Loss: 0.30dB(max)
Operating Temperature: -40°C to +75°C
Outdoor F/O Cable, Loose Tube, SM OS1/2–1x6 Fibres, Steel rod with CST, PE
The fibre should be optimized for operation at 850 nm and at 1300 nm.
Should fulfil the requirements of ISO.IEC 11801 – 2nd Edition, type MM OM4, ITU-T REC G 651D spec IEC 60794-1-2 F5
No of Cores: 6
Max. Attenuation: At 850 nm <= 3.0 dB/km, At 1300 nm <=1.0 dB/km
Attenuation: 1310/1550: 0.36/0.22 dB/KM
Fibre/Tube Identification: Single Tube
Fibre protection (Tubes): Polybutylene Terephthalate (PBT)
Armouring: CST
Outer Sheath: HDPE >2.0 mm
Peripheral Strength Member: 2 nos of Steel rod
Cable Diameter (D): 8.8 ± 0.3 mm
Mass (Nominal): 82 kg/km
Min. Bending Radius (during Installation): 20 D; D-Outer Diameter
Max. Tensile Strength-Short Term: 1500N
Max. Crush Resistance-Short Term: 3000N
Operating Temperature range: -40°C to +70°C
Fibre-Optic LIU Rack Mount LIU (12-Ports)
Should supports up to 6/12/24 duplex SC/LC adapters (12/24/48 fibres)
Pull-out drawer enables ease of access to the fibre
Height: 1 U, 1.75 inches rack mounting brackets allow for recessed panel mounting, enhancing cable protection
Rear cable entry cut-outs including one cable entry gland
There should be moving tray that provides built-in cable management by holding and arranging the cables
H: 44 mm / 1.72” (1U); W: 483 mm / 19”; D: 200 mm / 8” (face to rear); Weight:2.6 kg
Materials: Steel: Colour: Black with white silk-screened markings
12-Port SC/LC Type Adaptor & Plates (Single mode)
High performance single mode connectors and adapters
Push-pull coupling for easy insertion and high repeatability
High system durability, stability and repeatability
Precision adapters with rugged phosphor-bronze alignment sleeves
PC and precision APC ferrules for single mode applications
PC ferrules: Insertion Loss < 0.3 dB typical; Return Loss > 26 dB typical

Should be designed to NTT-SC standards
Design, should provide non-optical disconnect terminations in a push-pull coupling mechanism, has been tested to the rigorous Bellcore 326 standards
Temperature range: storage &operating -40°C to +80°C
Stability: 0.11 dB; Impact: 0.2 dB; Drop: < 0.3 dB

8.13. Testing

8.13.1. Final Acceptance Test

A. The acceptance of the Data Centre including DC site in accordance with the requirements shall be conducted. After successful testing of the features, facilities, functionalities and integrity of the commissioned devices, equipment and services by the PMO/AGCL, a Final Acceptance Test (FAT) Certificate shall be issued by AGCL to the System Integrator. The date on which Final Acceptance certificate is issued shall be deemed to be the date of successful commissioning of the DC. The FAT certificate will be signed by the System Integrator, PMO Consultant and AGCL.

B. The test shall include the following:

C. All civil, electrical, air conditioning works, etc., are completed as per the RFP specifications and solution documents proposed by the System Integrator and accepted by AGCL

D. All hardware and software items must be installed at DC site as per RFP specifications and solution documents.

E. Availability of all the defined services shall be verified (by whom). The System Integrator shall be required to demonstrate all the features/facilities/functionalities as mentioned in the RFP and solution documents.

F. The SI shall submit the test plan and the same should be approved by AGCL/PMO

G. System Integrator will arrange the test equipment's required for performance verification and also provide documented test results.

H. The System Integrator shall be responsible for the security compliance of the ICT infrastructure and network before the final acceptance test.

I. All documentation as defined in the RFP should be completed before the final acceptance test.

J. The training requirements as mentioned should be completed before the final acceptance test.

8.13.2. Hosting the ERP System

AGCL/ ERP Solution provider will host the proposed ERP solution at AGCL Data Centre set up by SI (bidder). It will also host the ERP application in the DR site/cloud.

8.14. Training and Change Management

8.14.1. Training and Capacity Building

A. The SI will to have identify/select and subsequently provide operational training to coreIT team of AGCL/ERP solution provider to operate the infrastructure (Around 20-30 nos. of people)

B. The SI will have to prepare a detailed training plan to impart the training and the same should be approved by AGCL.

C. It shall be the responsibility of SI to ensure that all the personnel that undertake the training have required proficiency and the same should be substantiated by a feedback exercise post completion of training.

D. The SI shall conduct onsite training after installation and commissioning has been completed. Training shall be provided for the entire scope of work. All the training material and other associated expenses shall be borne by the SI. The training shall cover both IT and Non-IT components.

E. The training course and materials should be in line / equivalent to the OEM's syllabus for professional certifications. The training should be OEM certified instructor led and should be conducted by the respective OEMs at Duliajan.

F. All the OEMs should give hands on training on their products to the O&M team and well as AGCL/ERP team.

The indicativetopics for training are as below:

Sl. No.	Training Description
Non- IT Training	
1	Data Centre Design
2	Overview of Non-IT Components
3	Electrical Distribution System
4	DG System & Operation
5	UPS System & Operation
6	Safety Security System & Operation
7	Data center structured Cabling solution
8	All others remaining details of Data Center
IT Training	
9	Overview of IT Components
10	Data Centre IT Architecture , Data Centre Network Design
11	Enterprise Storage Systems Architecture
12	Enterprise Management Systems
13	Cyber Security Components
14	L1 training for network equipment's, Servers, Operating Systems, Databases, Security equipment's
SLA	
15	Overview of SLA Monitoring & Management
Do's & Don't	

G. The above table is just minimum indicative list, type of training to be provided, however, it is required to furnish the training details along with the time period and each types of training, the target audience for the respective training and the number of people that should attend the training.

In addition, the bidder has to ensure that:

The AGCL team is familiarized with the existing configuration of the Data Centre and follow the guidelines for operation.

The AGCL team should have the basic and effective knowledge on how the facility operates as per the implemented design. This involves network connection, power, cooling and support.

Bidder shall provide all necessary training to AGCL officials and authorized team members for the purpose of successful functioning of the Data Centre operation and management.

8.14.2. Operation and Maintenance

A. Following are the summary of operations and maintenance services to be provided by the Bidder to be performed under the supervision of AGCL.

B. Bidder shall provide comprehensive technical support services for all the hardware and software proposed for the entire period of the contract. The technical support should include all the upgrades, updates and patches that are released by the respective OEMs during the period of contract.

C. Bidder shall provide comprehensive onsite warranty on all the equipment for a period of 5 (Five) years from the date of Go-Live of all IT infrastructure provided as part of scope of this tender.

D. The onsite warranty should also include all the upgrades, updates, major or minor patches that are released by the respective OEMs during the period of contract.

8.14.3. Technical Support Desk

Technical Support desk shall undertake the following activities:

- Log issues / complaints related to IT infrastructure at the Data Centre and issue an ID number against the issue / complaint.
- Assign severity level to each issue / complaint so as to maintain categorization and differentiate the criticality of the incident via the priority levels, severity levels and impact levels
- Track each issue / complaint to resolution.
- Escalate the issues / complaints, to AGCL officials if necessary.
- Analyze the issue / complaint statistics and bidder's SLA
- Should provision for all necessary channels for reporting issues to bidder's/OEM technical team. The incident reporting channels will be the following
    - Email
    - Telephone (mobile phone alerts)

Should implement a call logging system in line with the severity levels as mentioned in the SLA.

9. Project Timeline and Payment Schedule

9.1. Project Timelines for Implementation

AGCL intends to complete the ICT Installation and Commissioning in 5 months. "T0" refers to the project initiation date. However, the bidder has to provide support after installation and also perform commissioning activities during Go-Live/ Stabilization and maintenance and onsite warranty during Warranty phase

AGCL intends to complete the Data Center implementation by 5 months.

Sl. No	Description	Timeline
1	Project Kick off	T
2	Site readiness in terms of civil, electrical, Networking, and other security parameters	T+ 4 weeks
3	Delivery of Hardware at the Data Center at AGCL and installation and commissioning of the same	T+10 weeks
4	Data Center Up and Running along FAT and UAT	T+16 Weeks= T_0
5	Training of AGCL Staffs and Go-Live of the Solution post Implementation of ERP by ERP Solution Provider	T_0+16 weeks= T_1
6	Support and Maintenance Phase	T_1 + 5 years

Note:

A. The time schedule mentioned above is indicative and will be finalized by mutual agreement and discussion between AGCL and the successful bidder.

B. Initially, Bidder will provide draft deliverable to AGCL for their review and feedback within stipulated timelines.

C. AGCL will provide feedback to make necessary changes, corrections, if required. Bidder will be required to resubmit the revised document/deliverable.

9.2. Payment Schedule for Implementation

Payment will be released to the successfully shortlisted bidder in phased manner as stated below:

Deliverables/Milestones	Payment	Remarks
Inception Report / Mobilization Advance	5 % of total capex quoted value	Submission of Design document, drawings, coordinated drawings, Project plan, Resource deployment plan, Engagement of Project Manager at site.
Execution of major civil, interior works, safety & security systems and passive network cabling works electrical, Networking and security works	10 % of total capex quoted value	Supply and Installation of Brick work, PCC flooring, Partition work, indoor conduit and cabling work for lighting, raw power and UPS points cabling, Earthing and Grounding work, Networking, Band-width provision, CCTV installation etc and all safety & security
Commissioning & Testing of all Non-IT systems (PAT of Non-IT System) and Supply & Installation of major IT components	45 % of total capex quoted value	Supply & installation of Hardware like servers,network devices, storage, firewall, cybersecurity devices and all other IT devices without licenses
Commissioning & Testing of all IT systems, and software solutions (PAT of IT System).	30 % of total capex quoted value	Supply and installation of endpoint security licenses, and other software licenses.
Final Acceptance Test & Go-Live of DC. Engagement of Operation & Maintenance team	10 % of total capex quoted value	Final Testing and commissioning of individual systems and components, Integrated testing, Go-Live certification and Engagement of Operation and maintenance team
Operations and maintenance Management for 5 year payable quarterly	25% (per quarter- (QGR)) of the yearly quoted price.	Payment terms would be quarterly in arrears after making due adjustment with SLA/ performance

Note: -

A. All the payments will be made to the successful bidder in Indian Rupees only. Paymentswill bemadeafterthirty(30)daysofreceivingtheinvoicesubjecttoapprovalfromcompetentauthority. The billing has to be made in the name ofAGCL.

B. Tax shall be shown extra by the Bidder in their invoices for the items applicable. The same shall be paidbyAGCLasperactualafterverification.Similarly,ifthereisanytaxsavings,thesameshallbe reduced from the payableamount.

C. In case of any new incidence of tax or any change in existing tax rates taking place during the Agreement Period, that shall be borne and payable by AGCL over and above the agreed price for each item as may be applicable as per the Invoice raised by either Party/Member of the on AGCL. Similarly, any reduction in taxes shall be to the benefit of AGCL. All invoices produced to AGCL for payment should be with TAX invoice.

D. The percentage of the operational expenditure (OPEX) should not be less than 35% of the total quoted value.

E. **CAPEX** may include the cost of Non-IT, IT equipment, active and passive component required for AGCL (Year 0 Cost).

F. **OPEX** may include operational expenditure as Manpower cost, and Annual maintenance cost of all the equipment's for 05 (Five) years (Year 1+ Year 2+ Year 3+ Year 4+ Year 5) etc. to be incurred by the bidder for operation and maintenance for 5 years after Go-Live.

10. Service Level Agreement and Penalty

10.1. Service Level Agreement and Penalty

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof to be offered by Bidder to AGCL. The Bidder shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels to provide quality services. The Bidder shall meet service level objectives and corresponding parameters to ensure the delivery and quality of services on time as per standard mentioned in the document. Service level indicators & and the target performance levels to be maintained by the Bidder during the contract period. SLA shall be strictly imposed and agency shall be deployed for reporting the performance of the Bidder against the target performance metrics. All logs, reports and data that shall be made available for the purpose of evaluation/audit of SLA parameters/target performance metrics should be system generated only.

The benefits of this SLA are to:

- ✓ TriggeraprocessthatappliesCustomerandtheBiddermanagementattentiontosomeaspect of performance when that aspect drops below an agreed upon threshold, ortarget.
- ✓ Makes explicit the expectations that Customer has forperformance.
- ✓ Helps Customer to control the service level and performance of Bidderservices.

The Bidder shall have to submit a quarterly report to monitor the performance of the servicesbeing provided by the Bidder and the effectiveness of thisSLA

10.2. Brief Description of the Services to be provided

The Bidder will provide following services for Site Preparation & Supply, Installation and Maintenance of basic Infrastructure for the establishment of State Data Centre at the proposed site. The exact scope and boundaries of services provided as part of this Contract are detailed in Detail Scope of Work therein of this RFP.

- ✓ Site Preparation of the proposed Data Centre in terms of the civil, electrical and mechanical work required to Build and maintain the DataCentre.
- ✓ Supply,installationandsettingupofthenecessarybasicInfrastructure(stateofArtUPSand Transformer,Firemanagement,Lightingsystem,FireDetectionand Control system, Structure Cabling,etc.).
- ✓ Supply, installation and setting up of the physical security system and CCTV surveillance systems.
- ✓ Five years on-site maintenance of all the equipment's and their components suppliedin setting up the basic Infrastructure in the proposed Data Centre.
- ✓ Onsite support for Data Centre Infrastructure Operations on **Standard Business Hours of AGCL** basis by skill manpower / Personnel for a period of five years to ensure 99.982%availability

10.3. SLA Definitions

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings set forth below:

- ✓ **"Availability**"shallmeanthetimeforwhichtheservicesandfacilitiesofferedbytheBidders are available for conducting operations from the equipment hosted in the DataCentre.
- ✓ "**Downtime**" is the time the services and facilities are not available to Customer, which excludes the scheduled outages planned in advance for the DataCentre.
- ✓ "**HelpdeskSupport**"shallmeantheBidder's**Standard Business Hour**HelpdeskSupportCentrewhichshall handle Fault reporting, Trouble handling, Ticketing and related enquiries during thiscontract
- ✓ "**Incident**" refers to any event / abnormalities in the functioning of the Data Centre Equipment / Services that may lead to disruption in normal operations of the Data Centre services.
    - o **CRITICAL (L1)**: Incidents, whose resolution shall require additional investment in component or time or shall involve coordination with OEMs. These incidents shall impacttheoverallfunctioningoftheDC.Forexample,Powerfailure,failureofSpine switch,etc.
    - o **Medium (L2)** : Incidents, whose resolution shall require replacement of hardware of software parts, requiring significant interruption in working of that individual component,forexample,installationofoperatingsystem,replacementofswitch,etc.
    - o **Low (L3)** : Incidents, whose resolution shall require changes in configuration of hardware or software, which will not significantly interrupt working of thatcomponent.
- ✓ "**ResolutionTime**",meanstimetakenbytheBidderstafftotroubleshootandfixtheproblem from the time the call has been logged at the Helpdesk till the time the problem has been fixed.

10.4. Category of SLA

ThisSLAdocumentprovidesminimumlevelofservicesrequiredaspercontractualobligations based on performance indicators and measurements thereof. The DCO shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performancelevels.

The SLA has been logically segregated in the following categories:

A. Performance Related ServiceLevel
B. IT infrastructure related servicelevel.
C. Security and IncidentManagement
D. Helpdesk SupportServices
E. Manpower related ServiceLevel
F. Compliance & ReportingProcedure

10.5. Targets of Service Level Agreement

SLA clause provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Bidder shall ensure provisioning ofall requiredserviceswhilemonitoringtheperformanceofthesametoeffectivelycomplywiththeperformanc elevels.TheservicesprovidedbytheBiddershallbereviewedbytheConsultant/PMU and Customershall:

- ✓ Check performance of the Bidder against this SLA over the review period and consider any key issues of the past period's performance statistics including major incidents, service trends, etc.
- ✓ Discuss escalated problems, new issues and matters still outstanding forresolution.
- ✓ Review of statistics related to rectification of outstanding faults and agreedchanges.
- ✓ Obtain suggestions for changes to improve the servicelevels.

In case desired, Consultant /Customer may initiate an interim review to check the performance and the obligations of the Bidder. The SLA may be reviewed and revised in accordance to the defineprocedures.TheproceduresswillbeusedifthereisanydisputebetweenCustomerandthe Bidder on what the performance targets shouldbe.

10.6. Performance Related Service Levels

S No	Measurement	Definition	Interval	Target	Target in Time	Penalty
1.	Data Centre Availability	Availability = {1-[(Downtime) / (Total Time – Maintenance Time)]}*100 Availability of Power will be measured up tothe socket level in the equipment room that will be providing power to the racks.	Quarterly	>= 99.98%	25 minutes Continuous downtime	No Penalty
				>= 99.75% to <99.98%	<= 30 minutes to > 25 minutes of downtime	0.5% of the QGR value
				< 99.75%	> 30 minutes of downtime	For every 0.25% reduction in the uptime there will be a penalty of 2% QGR.

10.7. IT Infrastructure Service Level

IT Infrastructure service level will be applicable on the devices which are part of the BOM.

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	IndividualServer Availability (including the OS, database and the	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGRvalue for O&M of IT system

Sl. No.	Definition	Measurement Interval	Target	Penalty
	application running onit)		< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning maybe issued to the bidder.
2	Storage Availability	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGRvalue for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning maybe issued to the bidder.
3	Managed Backup Service Availability (with agreed retention period) Managed Backup Service provides automatic scheduled backup of Customer Data to the designated storage vault 'as is where is' and also restore it back in the same format as backed-up. Data backup Success Ratio must be calculated.	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGR value for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning maybe issued to the bidder.
4	Connectivitywith Internet (With regards to DC equipmentonly)	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGRvalue for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter of warning maybe issued to the

Sl. No.	Definition	Measurement Interval	Target	Penalty
				bidder.
5	LAN availability (Active and passive components)	Quarterly	>=99.98%	No Penalty
			>= 99.97% to <99.98%	0.1% of the QGR value for O&M of IT system
			>= 99.96% to < 99.97%	0.25% of the QGR value for O&M of IT system
			>= 99.93% to < 99.96%	0.5% of the QGRvalue for O&M of IT system
			< 99.93%	1.0 % of the QGR value for O&M of IT system [Record as Event of Default] Letter ofwarning may beissued to the bidder
6	Preventive Maintenance DCO shall provide a detailed Preventive maintenance plan/Schedule on commencement of the Project.	Quarterly Reporting	100%Carried Out. PM Plan shouldbe Approved from PM, AGCL prior to be carried out in thatquarter.	2% of the QGR value for delay in PM activity. 0.1% of the QGR value for non-adherence to PM plan or withoutapproval. If PM of any equipment missed in a quarter, the same should be carried out within next two weeks. Else penalty of Rs. 5000/- per day per equipment for delayswill be deducted.

10.8. Security and Incident Management Service Levels

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	For every Virus attack reported and not resolved within 36 hrs from the time of attack	Every instance in the Quarter	Beyond 36 hrs	Rs.20,000.00 for delayof every 24 hours or its part. If more than three virus attacks are reported in a quarter, then 10% of the QGR would be deductedas penalty.
2	For every instance of Denial of Service (DoS) attack and not resolved within 2 hrs from the time of attack.	Every instance in the Quarter	Beyond 2 hrs	Rs.5,00,000.00 per DoS attack
3	For every instance of Data Theft, the bidder is subject to penalty and/or punishment applicable under the IT act/ AGCL data theft policy or any other prevailing laws of the State/Country at that point of time, which shall be over and above the stated penalty.	Every instance in the Quarter	At every instance	Rs.5, 00,000.00 per instance.
4	For every Intrusion reported by firewall or IPS and not resolved within 2 hour from the time of report	Every instance in the Quarter	Beyond 2 hrs	Rs.2,00,000.00
5	Patch Management (including rules updation in Firewall, IPS and updation of any SPAM control policy)	Every instance in the Quarter	Within 2 hrs time from the approved Request	No Penalty
			> 2hrs and <=3hrs	Rs.1,00,000.00
			> 3hrs and <=4hrs	Rs.2,00,000.00
			> 4hrs and <=5hrs	Rs.3,00,000.00
			Beyond 5hrs for every 3 hrs	Rs.5,00,000.00

10.9. Help Desk Support Services Level

Response time: is defined as the time between receipt of the incidence (helpdesk call/ receipt of alarm generated by management system) and a support team member begins working on the incidence.

Resolution time: is defined as the total time between receipt of the incidence (helpdesk call/ receipt of alarm generated by management system) and the incidence been resolved.

Service Window:

A. PWH (Prime Working Hours): 8AM to 5 PM (Monday to Saturday)

B. EWH (Extended Working Hours): 5 PM to 8AM (Monday to Saturday), Sunday and all state Government Holidays.

Priority	Response Time	Resolution Time		MAT (Maximum Allowable Time) After Resolution Time.	
	PWH or EWH	PWH	EWH	PWH	EWH
L1	10 minutes	Within 6 Hours	Within 6 Hours	4 Hours	4 hours
L2	20 Minutes	Within 8 hours	Within 12 hours	4 hours	4 hours
L3	30 Minutes	Within 12 hours	Within 24 hours	12 hours	12 hours

S NO	Definition	Measurement Interval	Target	Penalty
1.	**"Resolution Time"**, means time taken by the Bidder staff to troubleshoot and fix the problem from the time the call has been logged at the Helpdesk till the time the problem has been fixed.	Quarterly	100% calls to be resolved within 30 minutes	No Penalty
			Calls resolved after 30 minutes ofOR Unresolved call	0.01% of the T otal QGR value for every call (with the delay of 30 minute) on an incremental basis.

Setting Priority Level

The Helpdesk at AGCL will make every effort to resolve issues at the time of the service call. This will be the initial method for resolving issues before assigning a priority level. Helpdesk staff will log and assign priorities for all requests not resolved at the time of the call.

Incident priority is primarily formed out of its Impact and Urgency. The helpdesk will maintain a matrix as per the EMS deployed which will automatically calculate incident severity out of the simple value of Impact x Urgency.

Impact of the incident is the measure of how business critical it is. Urgency is a necessary speed of resolving an incident.

Priority = Impact x Urgency

10.10. Manpower Service Levels

Sl. No.	Definition	Measurement Interval	Target	Penalty
1	Resource availability for all services agreed for Operation andMaintenance purpose of the project.DCO	Quarterly	Single absence of a single resource	No Penalty (if replaced by equivalent skilled resource)
	manpower should be available Business hours and Business days.			Replacement should be subject to prior approval of Project Manager AGCL
				Double of the cost of the absent resource for the period of absence.

NB: Minimum no of Resource need to be present in all shift at Data Centre should be not less than 8. (Excluding Holidays)

A. The replacement of manpower by bidder after deployment will be allowed (without penalty) only in below cases.

B. Theresourceleavestheorganizationbysubmittingresignationwithpresentemployerandacopy of resignation should be marked to AGCL.

C. Bidder will withdraw the resource as per its own organization policy in case of non-performance and non-corporation in line with the AGCLguidelines.

D. For Skills and Competence level the resource profile, educational qualification and certifications should be verified by the Consultant and AGCL jointly prior todeployment.

E. No resource will be absent without prior permission from the designatedauthority.

F. ABackgroundVerificationmaybecarriedoutforselectedresourcestoensurenocriminalhistory present.

Details of manpower requirement is as follows:

Sl.	Role	Working Shifts			
		6:00 AM To 2:00 PM	10:00 AM To 5:00 PM (Monday to Saturday)	2:00 PM To 10:00 PM	10:00 PM To 6:00 AM
1	DC Project Manager	☎	1	☎	☎
2	Network & Security Administrator	☎	1	☎	☎
3	Server Administrator	☎	1	☎	☎
4	Database Administrator	☎	1	☎	☎
5	Storage and Backup Specialist	☎	1	☎	☎
6	SIEM Analyst	☎	1	☎	☎
7	Network Engineer	1	-	1	1
8	Server Engineer	1	-	1	1
9	Helpdesk Support	1	-	1	1
10	Facility Manager	☎	1	☎	☎
11	Electrical Supervisor	☎	1	☎	☎
12	FrontDesk Executive	-	1	-	-
	Total	**8**	**14**	**8**	**6**

Note:

- Above manpower requirement table is indicative as minimum requirement for AGCL
- Bidder should have their enough additional resource to meet the challenge of leave/replacement/changes for smooth delivery ofservices.
- General shift shall be considered as 8:00 AM to 05:00 PM excluding all state govt. holidays and nationalholidays.
- IT manpower (except Helpdesk Executive) & key Non-IT resources mentioned in resource table must be a payroll employee of the successful biddercompany.

10.11. Compliance & Reporting Procedures

S NO	Measurement	Definition	Measurement	Target	Penalty
1	Submission of MIS Reports and SLA reports	The Bidder shall submit the MIS reports and SLA reports Quarterly and as and when required to the AGCL	Quarterly	Report for the previous quarter shall be submitted within the first week of next quarter.	No Penalty
				Delay beyond the date of submission	0.01% of the QGR value for every week time delay
2.	Incident Reporting	Any failure/incident on any part of the Data Centre infrastructure or its facilities shall be communicated immediately to Customer as an exceptional report giving details of downtime, if any.	Quarterly	100% Critical incidents to be reported to Customer within 1 hour with the cause, action and remedy for the incident.	No Penalty
				Delay beyond an hour	1% of the QGR Payment for every hour's delay on an incremental basis.
3.	Change Management	Measurement of quality and timeliness of changes to the Data Centre facilities	Quarterly	100% of changes should follow formal change control procedures. All changes need to be approved by Customer. It should be implemented on time and as per schedule & without any disruptionto business	0.1% of the QGR value for every non-compliance of Change request on an incremental basis.

4.	Scheduled Maintenance	Measures timely maintenance of the equipment installed at the Data Centre. The Bidder shall provide a detailed equipment maintenance plan on the commencement of the project.	Quarterly	100 % of scheduled maintenance should be carried out as per maintenance plan submitted by the Bidder. Any scheduled maintenance needs to be planned and intimated to Customer at least 2 working days in advance	0.1% of the QGR Payment for every non-compliance on an incremental basis
5.	Maintenance of Inventory	The Bidder should maintain an inventory of items that will be required on an ongoing basis for maintenance	Quarterly	100% as per the inventory log committed and maintained by Bidder.	0.1% of the QGR Payment for every noncomplian ce

10.12. Penalty

A. Penalty Capping:

Note: Equipment Availability Related penalties shall be governed by the following conditions:

1. The penalty shall be calculated on QGR as per the SLAdefined.
2. The total quarterly deduction should not exceed 20% of the total applicable fee in aquarter.

B. Penalty for Non-Measurable of QGR Parameters:

The below penalty will not be included in the maximum overall QGR penalty of 20% enforced on DCO. However, in case of non-measurable of any of the two QGR parameters mentioned below, then maximum penalty of 10% or 10% plus Non-Measurable Parameter Penalty which ever will be more will levied onDCO.

I. For not measurable of Security and Incident Management SLA's. Penalty of Rs. 50,000/- would be enforced onDCO.

II. For not measurable of IT Infrastructure related SLA's. Penalty of Rs. 50,000/- would be enforced on DCO.

III. For not measurable of Physical Infrastructure related SLA's. Penalty of Rs. 50,000/- would be enforced on DCO.

IV. For not measurable of Major and Minor Civil/ Electrical Works SLAs. Penalty of Rs. 25,000/- would be enforced on DCO.

V. For not measurable of Helpdesk Services. Penalty of Rs 50,000/- would be enforced on DCO.

VI. For not measurable of Compliance and Reporting SLA's. Penalty of Rs. 50,000/- would be

enforced on DCO.

VII. For not measurable of Manpower Availability. Penalty of Rs 50,000/- would be enforced on DCO.

10.13. Exclusion

The penalty will not be applicable, in case of non-availability of the Force Majeure invocation.

10.14. SLA Change Control

It is acknowledged that this SLA may change as Customer's business needs evolve over the course of the contract period. This document also defines the following management procedures:

A. A process for negotiating changes to the SLA and methodology.

B. An issue management process for documenting and resolving difficult issues.

Customer and Bidder management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

Any changes to the levels of service provided during the term of this Agreement will be requested, documented and negotiated in good faith by both parties. Either party can request a change. Changes will be documented as an addendum to this SLA and, subsequently, the SLA methodology and the Contract.

10.15. SLA Change Process

A. The parties may amend this SLA by mutual agreement in accordance with terms of this contract. Changes can be proposed by either party. The Bidder can initiate an SLA review with the Customer.

B. Normally, the forum for negotiating SLA changes will be Customer's meetings with consultant.

C. The Bidder shall maintain and distribute current copies of the SLA document as directed by Customer. Additional copies of the current SLA will be made available at all times to authorized parties.

10.16. Warranty Phase Payments

A. The SI/Bidder shall make a payment request after the end of each quarter with documents i.e., (a) Invoice in triplicate (c) SLA compliance report.

B. Upon receipt of request from the SI/bidder, invoice will be processed, and payment will be released within 15 working days from the date of receipt of request after accounting for deductions on-account of SLA and other penalties / recoveries.

11. Maintenance Support

11.1. Commissioning of System

A. Bidder should describe in advance the tests and details of the process that will be adopted to demonstrate the correct working of the equipment supplied both individually and as an integrated system.

B. System testing schedules, formats for testing and commissioning reports and dissemination mechanism for such reports shall be drawn by the Bidder in consultation with AGCL

C. Commissioning of the solution shall be considered to be complete only after the following conditions have been met successfully to the satisfaction of AGCL.

   a. Successful completion of Factory Acceptance Tests and submission of necessary reports and certificates to AGCL.

   b. Delivery of all the items under the proposed bill of material at the designated locations of installation. Short shipment of goods will not be acceptable.

   c. Installation and Configuration of all the components of the solutions including, but not limited to, hardware, software, devices, accessories, etc. to the satisfaction of AGCL

   d. Successful completion of Commissioning post Go-Live would need to be certified by AGCL and operations shall commence only after approval of AGCL.

11.2. Policies and Procedures

An effective datacenter management strategy includes policies and procedures that needs to be documented and enforced to ensure that they are understood and followed as inconsistencies in the performance can lead to service interruptions or downtime.

Requirements:

A. Data Centre User Manual – This includes all information that is critical to run the Data Centre from construction phase to operation.

B. Data Centre Instructions – This are set of rules inside the Data Centre that prevents any risk to Data Centre operations.

C. Emergency / Crisis Management Plan – this is to ensure control and management inside the Data Centre during an emergency or abnormal situations.

D. SOP's – Set of instructions or guide to operate DC configurations on normal conditions

E. Health & Safety Procedures – Set of HSE guidelines specifically for the Data Centre to prevent accidents or harm to the DC team or visitors.

F. Access Procedures - this access guideline specifies the criteria for granting access to specific individuals or groups, and the different levels of access allowed.

G. Maintenance Procedures – this specifies how a maintenance procedure is scheduled and performed.

11.3. Maintenance Management

A. An effective maintenance program is necessary to keep equipment in an optimum condition, minimize failures and prevent downtime. This includes preventive and predictive maintenance, strong vendor support, failure analysis, life cycle tracking and documentation. Any level of vendor support to maintain infrastructure should have a corresponding list of qualified vendors with formal

contracts specifying the scope of work, call-in process, qualifications, and response times to ensure the level of service required meets the uptime objectives.

B. The vendor needs to provide the following to ensure proper upkeep of Data Center post the 5-year warranty period by AGCL or its representative.

C. List of all equipment

D. Specialized Vendor Details – This contains the details of the vendor(s) assigned to maintain DC equipment. Technician information, qualifications and certifications should be available.

E. Service Level Agreements – Should clearly define the Response Time and Conditions to match our requirement as well as OEM recommendations.

F. Planned Preventive Maintenance (PPM) – PPM schedule should be fixed for the entire period of contract. So AGCL can plan other activities accordingly without conflict.

G. Sequence of Operation – This shows the operation of any equipment with redundant functionality in case of a primary source failure. Example: UPS, Generator, Etc.

H. Escalation Matrix or Emergency Call-out Matrix – This allows to clearly identify the response team responsible for any equipment failure

I. Service Evaluation – This is to evaluate the assigned team and request for changes if required. This will increase the quality to the support from the service team.

J. Methodology and Risk Assessment – This is to provide information on how the maintenance will be performed and the risk that comes with it. This is required for all maintenance activities – may it be major or minor.

K. Critical Spare Parts - These are list of spare parts to be available at the nearest store of OEM to sustain operation of DC critical equipment. The vendor/bidder shall confirm as part of this RFP to maintain the inventory of critical spares at his end.

L. Predictive Maintenance – This will allow the team to alter PPM schedule to match the equipment maintenance as required.

M. Additionally the bidder should provide a comprehensive maintenance support/warranty on all the equipment installed, including cabling etc. for 5 years from the date of Go-Live/Acceptance of Datacenter Solution whichever is later.

N. No Objection Certificates (NOC) – This is to allow any new requirement or projects directly impacting Data Centre operations.

O. Change Request Forms (CR) – This is required for any major modification or change request on the existing setup of the Data Centre. This also covers revoking access permissions to existing permanent users.

11.4. Documentation

These are set of references or records provided on paper or on digital media. These documents act as the store of collective organizational and operational knowledge regarding the processes and can be accessed by anyone in times of need. All these documents should be latest, updated, protected and available.

The bidder will have to provide the following minimum Documents to AGCL at the start of Warranty.

A. Asset list – list of equipment installed for Data Centre operations.

B. As-built drawings – final approved layouts as installed before activation. This is used as basis and includes civil, electrical, IT, Non-IT, and passive components.

C. Licenses – licenses for all IT, Non-IT, applications, databases and passive components (wherever applicable) should be made available for support and service.

D. Operation manuals – used as reference for the equipment functions.

E. Procedure manuals – used as reference for the specified OEM procedures.

F. Data Sheets – reference for equipment specification.

G. Equipment Set Points – reference for equipment configuration.

H. Testing and Commissioning Procedures – verifies proper operations of systems via documented testing procedures and establishes performance criteria in line with OEM standards.

I. Warranty Certification – an effective warranty management program secures operational stability through knowing the limits and exceptions of the product as per OEM. This includes all electrical, IT, Non-IT, and passive components (wherever applicable) and should be made available for support and service.

11.5. Reports

Consolidated component-wise ICT infrastructure availability and resource utilization report as mentioned below has to be submitted to AGCL in hardcopy as well as in softcopy by the bidder:

Monthly Reports/Quarterly Reports

A. The bidder has to submit a minimum of below reports on both monthly and in consolidated form on a quarterly basis.

    a. Component wise IT infrastructure availability and resource utilization.

    b. Consolidated SLA / non-conformance report.

    c. Summary of issues / complaints logged at the Technical Support desk

    d. Summary of resolved, unresolved and escalated issues / complaints

    e. Issues / Complaints Analysis report for virus calls, call trend, call history, etc.

    f. Summary of systems rebooted.

    g. Log of backup and restoration undertaken

    h. Summary of issues / complaints logged with the OEMs.

    i. Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

    j. Summary of component wise Data Centre uptime.

    k. Summary of changes in the Data Centre.

    l. Log of break-fix maintenance undertaken

m. Inventory of critical spare parts in the nearest stores.

12. General Conditions of Contract

12.1. Application

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

12.2. Standards

A. All the goods/services supplied under this contract shall conform to the standards mentioned in the Technical Specifications/Scope of Work and when no applicable standard is mentioned, to the authoritative standard appropriate to the Goods. All standards shall be the latest issued by the concerned institutions.

12.3. Contract Documents

The term "Contract Documents" shall include the following which will form an integral part of the contract:

A. Request for Proposal (RFP) and all its sections and sub sections including any corrigendum issued if any, Bidding documents, General Conditions of Contract and Special Conditions of Contract.

B. The specifications of products and services to be provided under this contract as laid out in the Scope of Work and Technical Specifications Section.

C. The proposal submitted by the bidder including all relevant documents attached there-to and any letter of clarification between the bidder and AGCL prior to award of contract.

D. All the materials, literature, data and information of any sort given by the Supplier/Contractor along with his bid, subject to the approval of AGCL.

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

12.4. Use of Contract Documents and Information

A. The supplier shall not communicate any information including but not limited to description of product, quality and quantity of product though any medium either written or visual without prior written approval from AGCL.

12.5. Manner of Execution of Contract

A. The selected bidder should send the signed copy of Letter of Intent (LoI) to AGCL within the prescribed timelines.

B. The Supplier/Contractor shall provide for signing of the Contract, Performance Guarantee, appropriate power of attorney and other requisite materials.

C. The Agreement shall be signed and have two originals and the Contractor/supplier shall be provided with one signed original and the rest shall be retained by AGCL.

D. The supplier shall provide free of cost to AGCL, at least 3 copies of all the descriptive materials submitted with the bid to form a part of the contract within 30 days after issue of Letter of Award.

E. Subsequent to signing of the Contract, the Contractor/supplier, at his own cost, shall provide AGCL with at least six (6) true copies of Agreement and one soft copy.

F. The Successful Bidder shall mobilize adequate resources for inception of the Project within fifteen (15) calendar days of issue of LoA by the Purchaser.

G. If the Successful Bidder fails to start the Project within the timeline mentioned in Section " Project Timeline and Payment Schedule" of the Bid Document, his Bid Security (EMD) will be forfeited and the Purchaser will have right to cancel the LoI/LoA and negotiate with the Bidder having second highest Final Score for placing the fresh LoI/LoA or invite fresh Bids.

12.6. Completion of Contract

A. This contract shall deem to have been completed on the date mentioned in the LoA, unless extended/terminated as per the terms of this RFP.

12.7. Time- Essence of Contract

A. The date of completion of contract as mentioned in the Letter of Award (LoA) and any modifications thereof shall be deemed the essence of the contract. It shall be the responsibility of the contractor to organize his resources and ensure completion of work as per the agreed timelines.

B. The contractor shall prepare a detailed project plan including a GANTT chart consisting of activities covering key phases of work as per the Scope of Work within 15 days of issuance of Letter of Award (LoA). The GANTT chart also needs to provide the interface facilities to be provided by AGCL along with the finalized dates by which such facilities shall be needed. The GANTT shall be approved by AGCL post discussions with the contractor.

C. The agreed and finalized GANTT chart shall form a part of the contract and will be utilized for monitoring the progress of the project. If at any time during the execution of project AGCL is of the opinion that proper progress is not maintained by the contractor, suitable changes shall have to be made by the contractor in its operations to ensure compliance to schedule.

D. Based on the agreed Bar Chart fortnightly reports shall be submitted by the Contractor to AGCL.

E. Subsequent to the finalization of the GANTT chart, it shall be the responsibility of the contractor to make available to AGCL, a detailed Work Plan as per the finalized GANTT chart. This Plan shall be reviewed and subsequently be approved by AGCL prior to implementation. The same shall be updated as per the actual progress of the project.

F. The Contractor shall provide AGCL both hardcopy and softcopy of the GANTT charts and Work Plan.

12.8. Extension of Time

A. AGCL may upon its sole discretion grant an extension of time for completion of the work, if it deems essential and for reasons as mentioned in the Force Majeure section which are beyond the control of the bidder subject to fulfilment of following conditions by contractors:

B. The supplier/contractor must apply to AGCL in writing for extension of time in writing so required justifying the necessity.

C. The application by the contractor should clearly state the grounds which hindered the contractor in the execution of work within the timelines as stipulated in the contract document.

D. The contractor shall submit such an application within 14 days of the date on which such hindrance had arisen.

E. AGCL should be convinced that the grounds shown for the extension of time are reasonable and without extension of such time, completion of the work is impractical.

F. The decision of AGCL in this matter shall be final and binding on the contractor.

12.9. Taxes, Permits and Licenses

A. It shall be the responsibility of the contractor to pay all non-Indian/Indian taxes, duties, levies lawfully assessed against AGCL or the Contractor in pursuance of the Contract.

B. AGCL shall have the right to deduct and adjust any amount which becomes payable by the supplier under particular contract and the same shall be deducted by the purchaser from any amount that is due or becoming due under the same or any other contract

12.10. Limitation of Liabilities

The final payment by AGCL including that of the O&M Contract period 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 AMC period as per the milestones defined in this RFP.

12.11. Change of Quantity

A. AGCL reserves the right to increase or decrease the quantities of items under the Contract but without any change in unit price or other terms and 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 ±10% of the contract value.

B. 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 period of the Contract. In case, the unit rates are not available for the change in quantity, the same shall be as per conditions of "Change of Scope" or finalized through mutual agreement between AGCL and Contractor.

12.12. No Waiver Rights of Agreement/Contract Provision

A. The failure of a party to insist upon strict adherence to any term of this Agreement on any occasion shall not be considered a waiver of such party's rights or deprive such party of the right thereafter to insist upon strict adherence to that term or any other term of this Agreement.

12.13. Certificate not to affect Right of AGCL and Liability of Contractor.

A. No interim payment certificate provided by AGCL, nor any sum paid on account of same by AGCL, nor any extension of time for execution of the Works granted by AGCL shall affect or prejudice the rights of AGCL against the Contractor or relieve the contractor of his obligation for the due performance of the Contract, or be interpreted as approval of the Works done or of the equipment furnished

B. In addition, no certificate shall create liability for AGCL to pay for alterations, amendments, variations or additional works not ordered, in writing, by AGCL 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 AGCL, nor shall any such certificate nor the acceptance by him of any sum paid on account or otherwise affect or prejudice the rights of AGCL against the Contractor.

12.14. Payment

A. Payment shall be made in accordance with Section "Project Timelines and Payment Schedule".

B. Any terms of advance payments i.e. payments against dispatch documents/Bank documents will not be acceptable.

C. In no circumstances, claim of interest on payment shall be entertained.

12.15. Settlement of Disputes

A. 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.

B. 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 as defined in the Scope of Work, 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 AGCL, who, within a period of thirty (30) days after being requested by Contractor to do so, shall give written notice of his decision to the Contractor.

C. Such decision shall be final and binding upon the parties until the completion of the Works.

D. If after the AGCL has given written notice of his decision to the parties, no claim to arbitration has been communicated to AGCL swithin thirty (30) days from the receipt of such notice, the said decision shall become final and binding on the parties.

E. In the event, contractor is dissatisfied with decision of AGCL, within thirty (30) days, after the expiry of the first mentioned period of thirty (30) days, as the case may be, it may move to arbitration proceedings to solve the dispute.

12.16. Arbitration

A. The parties will agree that the spirit of understanding and co-operation, which exists between them and is evidenced by the future MSA/Contract, is not indeed to create any legally binding obligations whatsoever upon either party, after decision of the referred RFP.

B. Any matter, whether or not stipulated in this RFP and later MSA/Contract, shall be settled in good faith by discussions between the parties in a spirit of mutual understanding & co-operation,

C. AGCL and the SI/Bidder shall make every effort to resolve amicably by direct informal negotiations any disagreement or disputes arising between them under or in connection with the Contract

D. If, after Thirty (30) days from the commencement of such direct informal negotiations, AGCL and the SI/Bidder have been unable to resolve amicably, then the unresolved dispute or difference shall be resolved by designated official from MeitY/NIC, GOI having knowledge of such Projects and shall be final and binding on all parties being co-signatory of this future contract

12.17. Conflict of Interest

A. The bidder shall ensure that has no business, professional, personal, or other interest, including, but not limited to, the representation of other clients, that would conflict in any manner or degree with the performance of its obligations under this Agreement.

B. If any such actual or potential conflict of interest arises under this Agreement, Contractor shall immediately inform the Company in writing of such conflict.

C. If, in the reasonable judgment of the Company, such conflict poses a material conflict to and with the performance of Contractor's obligations under this Agreement, then the Company may terminate the Agreement immediately upon written notice to Contractor; such termination of the Agreement shall be effective upon the receipt of such notice by Contractor.

12.18. End User Agreement by ICT OEM

A. In the event, AGCL is required to sign any end-user agreement with any OEM, any inconsistency between the terms and conditions as laid down in the contract agreement and the end-user agreement, the terms and conditions defined in this RFP and subsequent Agreement shall supersede

and the SI/OEM shall at its own cost / risk make compliance to such end-user agreement requirements without any additional cost / risk to the Purchaser.

12.19. Safety Rules

A. Each employee shall be provided with initial indoctrination regarding safety by the AGCL, 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 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. 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.

E. 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, the Contractors shall be responsible for payment of additional compensation over and above any other payment to the affected persons as per the compensation order issued by the appropriate authority of Government of Assam / verdict issued by court. . In case AGCL 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.

13. Special Conditions of Contract

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.

13.1. Subcontracting

A. No subcontracting is allowed as per the scope of this project

13.2. Technical Evaluation Criteria

A. Documents relevant for complying with various technical evaluation requirement are also to be a part of Contract Document

13.3. Execution of Contract

A. The Timelines to be followed for completion of this project shall be as per section "Project Timeline and Payment Schedule"

13.4. Duration of Contract

A. The contract with Qualified L1 SI shall remain valid for a period of 5 (five) years and 3 months from the date of signing of contract OR from the date of final acceptance testing whichever is later

B. The Warranty phase of the project will be 5 (five) years from the date of Go-Live of the project.

C. Go-live of the project will commence from the date of supply, installation and commissioning of equipment at 'AGCL-HQ, all 13 AGCL-Site offices (SO), and any other locations being identified by AGCL.

D. AGCL shall reserve the sole right to grant any extension to the term mentioned above on mutual agreement including fresh negotiations on terms and conditions

13.5. Causes for Extension of Time for Completion

A. The System Integrator may submit an application for an extension of the time for completion if he is of the opinion that he will be delayed in completing the Scope of Work by any of the following causes:

   i. Any changes in the Scope of Work in writing of any Additional work ordered there-of

   ii. Order for the suspension of work at the discretion of AGCL, received in writing for no fault on part of Contractor.

   iii. Force Majeure conditions as defined in Section Instruction to bidders.

B. For extension of time for completion, the SI shall give a written notice to the Purchaser of his intention to make a claim for an extension of time within fourteen (14) calendar days of occurrence of any of the above conditions. The notice shall contain all the supporting details for same.

C. The Supplier/ SI 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 SI shall not be entitled to an extension of time for completion, unless the SI has, at the time of such circumstances notified AGCL in writing, within the

prescribed timelines ,that it may claim such extension and upon request of AGCL the SI shall substantiate and prove that the delay is due the circumstances referred to by the SI.

E. AGCL, in its sole discretion may agree to extend the time of completion of contract as may be reasonable and mutually agreed but without prejudice to other terms and conditions of the Contract. However, the contract extension of time granted, if any by AGCL shall have no impact of the Contract price which shall remain firm and fixed.

13.6. Price Adjustment

A. The Contract price shall remain firm and will not be subjected to any upward revision/except as per the conditions contained in the "Change of Scope" during the entire 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.

13.7. Incident/Operational Expense Charges

A. The entire cost of project will be accounted in the price quoted by the bidder excluding relevant taxes. AGCL will not pay any extra charges/compensation incurred towards travel and lodging during the various phases of the implementation.

13.8. Modification

A. Any modification of this RFP shall be in writing and signed by an authorized representative of AGCL.

13.9. Relationship between Parties

A. Nothing in this Contract constitutes any fiduciary relationship between AGCL and SI/Bidder/SI/Bidder's Team or any relationship of employer employee, principal and agent, or partnership, between AGCL and the SI/Bidder.

B. All correspondence and documents pertaining to the Agreement that are exchanged by the parties shall be written in English language only.

13.10. Publicity

A. The SI/Bidder shall not make or provide his consent to make any public announcement or media release about any aspect of this Contract unless prior written consent of AGCL is obtained

13.11. Employees

A. Promptly and on reasonable request at any time during the Contract period, the SI/Bidder shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to AGCL a list of all employees (with job titles and communication address) of the SI/Bidder, dedicated to providing the services at AGCL offices/locations.

13.12. Right of Information Access

A. At any time during the Contract period, the SI/Bidder may be asked and will be obliged to provide access of information to AGCL, and/or any Replacement SI/Bidder in order to make an inventory of the Assets (including hardware / Software / Active / passive), layouts, diagrams, schematics, documentations, manuals, catalogues, archive data, IP addressing, Live data, policy documents or any other material related to AGCL Network Project.

13.13. Non-Suability

A. SI/Bidder cannot be sued in any court of law in India or abroad by AGCL /or Third-Party Auditor, for the events if Operator is not able to perform as per any of the stipulations of this agreement, due to circumstances beyond the control of it. Like–Power not available, Internet bandwidth not available, Backup power non-availability.

B. SI/Bidder cannot be sued in any Court of Law for being unable to provide any IT related support and failure, due to unforeseen circumstances or force majeure condition beyond control of SI/Bidder.

C. SI/Bidder cannot be sued in any court of law for any hacking, sabotage, cyber-attack, insider threats etc., Loss of Data (if any).

13.14. Indemnification

A. AGCL shall not be responsible for any payments, statutory obligation like insurance cover, PF, etc. for accident, mishap, handicap, and/or death occurring and affecting Operator /or it's Vendors employees or authorized personnel during and after the provision of the service at the POPs or client premises. Services include but are not limited to periodical inspection, installing, maintaining, replacing and removing equipment hardware, as well as to inspect the network. Operator shall not be held responsible for any downtime due to Internet Bandwidth, Diesel non-availability, Electricity Power, theft at-site, physical damage, cyber-attack, hacking, Force Majeure.

13.15. Confidentiality

A. SI/Bidder/AGCL/Third Party Auditor and their personnel shall not, either during the term or after the expiration of this contract, disclose any proprietary or confidential information relating to the services without the prior written mutual consent of the AGCL

13.16. Equipment Ownership

A. AGCL shall have all ownership of all the equipment and infrastructure once supplied at the AGCL-HO & SO by the SI/Bidder arising in-line with this RFP and subsequent Contract thereof.

B. The SI/Bidder can submit his Invoice once material is delivered at AGCL-HO and site offices duly signed and stamped for release of payment in-line with the payment terms of RFP and same will be released within 7 working days from the date of submission of the Invoices.

13.17. Information Security

A. The SI/Bidder shall not carry and/or transmit any material, information, layouts, diagrams, storage media or any other goods/material in physical or electronic form, which are proprietary to or owned by AGCL, without prior written permission from AGCL.

B. The SI/Bidder shall adhere to the Information Security policy of Government of India & as defined by AGCL.

C. The SI/Bidder acknowledges that AGCL business data and other AGCL proprietary information or materials, whether developed by AGCL or being used by AGCL pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to AGCL and SI/Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof. SI/Bidder may come into possession of such proprietary information even though SI/Bidder does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. SI/Bidder shall use such information only for the purpose of performing the said/required services for AGCL.

D. SI/Bidder shall, upon termination of this agreement for any reason or upon demand by AGCL, whichever is earliest return any and all information provided to SI/Bidder by AGCL including any copies or reproductions, both hard copy and electronic.

13.18. Statutory Requirement

A. During the tenure of this subsequent Contract nothing shall be done by the SI/Bidder in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof governing inter-alia customs, stowaways, foreign exchange etc. and shall keep AGCL indemnified in this regard.

B. The SI/Bidder and their personnel/representative shall not alter / change / replace any hardware component proprietary to AGCL and/or under warranty or AMC of third party without prior consent of AGCL.

C. The SI/Bidder and their personnel/representative shall not without consent of AGCL install any hardware or software not purchased / owned by AGCL

14. Formats for Eligibility Criteria

Annexure 1- Declaration of Eligibility Criteria

<<To be printed on lead bidder company's letterhead and signed by Authorized signatory>>

ELIGIBILITY CRITERIA FOR ICT Infrastructure

S.No.	Criteria	Submitted (Yes/No)
1	Bidder should be a registered Proprietary firm or partnership firm or private or LLP or Ltd. Company and a company incorporated in India under the Companies Act, 1956/Limited Liability Partnership Act 2008 and subsequent amendments and should be in existence for the last 8 years as on the date of issue of NIT in the areas of supply, implementation, operation and maintenance of Data Centre related ICT Infrastructure solution for large integrated solution such as ERP.	
2	Power of attorney / Board resolution in the name of the person signing the bid by Bidder	
3	Should have valid PF, IT, GST Registration Certificate.	
4	The Bidder should be an OEM certified/authorized System Integrator/Implementation Partner for the proposed Core ICT Infrastructure Hardware and Software Products. The System Integrator/Implementation Partner should have valid authorization/certification from the respective OEM(s) and have active relationship with the respective OEM(s). OEMs Authorization for Servers, Network equipment, Storage, Backup Solution, EMS, etc., are to be submitted.	
5	The Bidder should have an Average Annual Turnover of Rs. 150 Crore or more for last three (3) financial years ((FY 2017-18, FY 2018-19, FY 2019-20) with positive Net Worth for each of last three (3) financial years (FY 2017-18, FY 2018-19, FY 2019-20) from IT/ ITeS services / supplies	
5	Any direct Contract Agreement of the proposed bidder for ICT Infrastructure with AGCL should not have been terminated in last five (5) years.	

S.No.	Criteria	Submitted (Yes/No)
6	The Bidder shall not be under declaration of ineligibility for corrupt or fraudulent practices or blacklisted or debarred in last five years by any Department / Agency / PSU/ Organization of the Government of India or any State Government in India for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices.	
7	The Bidder should hold a valid ISO 9001:2015, ISO/ IEC 20000-1: 2011 and ISO 27001:2013. The certificate should be valid as on the date of submission of the bid	
8	The Bidder should have on its own payroll at least 150 technically qualified ICT Infrastructure professionals for providing technical services related to supply, installation, testing & commissioning followed by operation & maintenance of Data Center ICT Infrastructure, other ICT Infrastructure and associated packaged software, etc., out of which at least 30 employees should have minimum three (3) years of experience of working in data center environment and experience of successful implementation, operation and maintenance of data center ICT infrastructure including servers, Storage, Backup Solution, Data Center Networking, EMS Solution, etc.	
9	The Bidder should have a well-established presence in India with a support base to provide implementation and support for the proposed ICT Infrastructure solution & services along with the ability to provide timely response and service to the owner.	
10	The Bidder member should have a point of presence in the state of Assam or should open a Project Office within 30 days of receipt of Letter of Intent (LoI).	
11	The ICT Infrastructure solution- hardware OEM(s) whose products have been offered in the bid should be a registered firm or a company in India and should be in existence in India for last five (5) Years in the areas of selling of Data Centre related ICT Infrastructure solution(s), other ICT Infrastructure and associated packaged software, etc.	
12	OEMs of ICT Infrastructure solution whose products have been offered in the bid shall have SLA based local Technical Assistance Centers (TAC)/Support Center based in India with minimum 30 team members for offering post-sales support. OEMs should have its own TAC in India manned with its own engineers/professionals.	

S.No.	Criteria	Submitted (Yes/No)
13	The Bidder should submit valid authorization letters from each of the OEMs of the offered ICT Infrastructure related Product confirming that the products meet the technical & functional requirements asked for in the RFP document and that the Products quoted are of latest version / specification and are not at the end of sale, end of life and end of support.	
14	The offered products and the OEMs of any of the offered products should not be under declaration of ineligibility for any cyber security or information security threat by any Sovereign Government.	
15	The Bidder should have should have executed at least 1 project for IT Data Centre Implementation/ Maintenance with any Government / PSU Organization in India in last 5 years as on the date of submission of the bid: i. One similar project having the ICT Infrastructure component of total value of at least Rs 8 Cr (Eight Crore), OR ii. Two similar projects having the ICT Infrastructure component of total value of at least Rs 4 Cr. (Four Crore) each, OR iii. Three similar projects having the ICT Infrastructure component of total value of at least Rs.3 Cr. (Three Crore) each. Note:- Similar on-going/under implementation ICT Infrastructure projects shall be considered only in such cases where at least delivery and installation of the ICT Infrastructure for the required value have been completed.	
16	Bidder should have executed or in the process of executing at least 1 ICT project of value Rs. 4 Crore with any Government Organization in North Eastern State in India in last 3 years as on the date of submission of the bid.	

Signature of Authorized Signatory (with official seal) Name :

Designation :

Address :

Telephone andFax :

MobilePhoneNo :

E-mailaddress :

Annexure 2- Format for Bidder's Particulars

(To be printed on company's letterhead)

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Sl. No.	Description	Response
A	**General Information**	
1	Name of the Firm	
8	Type of Firm (Proprietary / Partnership / Private / Public)	
9	Year and Place of Establishment	
B	**Indian Operations**	
1	Head of Indian Operations	
2	Indian Head/Registered Office Address	
3	Name of the Contact Person	
4	Contact Number	
5	Fax Number (with ISD and STD Code)	
6	E-Mail Address	
7	Number of offices in India	
9	Net worth (for Indian operations) at the end of the last three financial years ending March 2020 (Please attach document certified by CA in practice)	
10	Annual revenue (from Indian operations) in the last three financial years ending March 2020	
11	Please attach copies of GST and PAN	
12	Number of full-time employees	
C	**Bank Information**	
1	Banker's Name	
2	Branch	
3	Branch Code	
4	Bank account number	

Contact Details of officials for future correspondence regarding the bid process:

Details	Authorized Signatory	Secondary Contact
Name		
Title		
Company Address		
Mobile		
Fax		
Email Id		

Yours Sincerely,

_____

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone and Fax :

E-mail address :

Annexure 3- Bidder's Annual Turnover- Last 3 Financial Years

To be printed on Company's letterhead

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Dear Sir,

IhavecarefullygonethroughtheTermsandConditionscontainedintheRFPDocument.Ihere by
declarethatbelowarethedetailsregardingOverallturnoveroverlast3financialyearsforour organization.

#	Details	FY 2017-18 (in Crores)	FY 2018-19 (in Crores)	FY 2019-20 (in Crores)	Average Turnover [(a+b+c)/3]
1	Overall Annual Turnover				
2	Sales turnover from ICT Business				

Yours Sincerely,

_____

Signature of Statutory Auditor (with official seal) Name :

Designation:

Address:

Telephone andFax:

E-mailaddress

Annexure 4- Declaration for not Being Blacklisted

(Self-declaration for not being blacklisted by any Government Entity)

(To be submitted on the Letterhead of the responding firm)

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Dear Sir,

This is to certify that we, (Name of the bidder) are not on Holiday list / debarred / blacklisted by any state or central government department nor by any state or centralPSU.

SIGNATURE AND SEAL OF BIDDER

Date:

Annexure 5- Format for Manufacturer's Authorization Form

To be submitted on the Letterhead of the manufacturer and duly signed by authorized signatory

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Ref: Tender No.: **XXXXX**

Whereas who are the official producers of and having production facilities at do hereby authorize located at (herein after "the Bidder") to submit the bid of following products produced by us, for supply requirement associated with the above Invitation for bids

Whenresoldby_____, these products are subject to our applicable standard end user warranty terms till the end of contract period by theSI/bidder.

We assure you that in the event of any failure/issue, not being able to fulfil its obligation as ourServiceProviderinrespectofthewarrantywewouldcontinuetomeetourwarrantythroug h alternatearrangements.

We alsoconfirmthat_____is our authorized service provider/system integrator and can hence provide maintenance and upgrade support for ourproducts.

We also confirm that the products quoted are on our current product list and are not likely to be discontinued within 5 years from the day of this letter. We assure availability of spares for the products for the next five years.

We also confirm that the License will be delivered within scheduled delivery dated as per the tender terms from the date of placement of confirmed order.

TheToll-freenumber,ticketingwebsiteandescalationmatrixwiththemailIdandfixedmobile number are as follows: _____

In case of any change it will be intimated to you immediately byus.

Name
In the capacityof
Signed
Duly authorized to sign the authorization for and onbehalfof _____

Datedon_____dayof_____2020

Annexure 6- List of Documents Submitted

Technical solution is to be presented in a structured manner. Checklist for the mentioned documents to be included in the technical bid in the following format:

#	Documents to be submitted by both SI and OEM (as per applicability)	Submitted (Y / N)	Documentary Proof (Page No.)
1.	Eligibility Criteria Cover letter (Annexure-1)		
2.	Power of attorney / board resolution to the authorized Signatory of the Bid on Non-Judicial Stamp Paper		
3.	Bidder's particulars (Annexure-2)		
4.	Bidder's annual turnover for last 3 years (Enclose copy of Audited Balance Sheet for last 3 years, Copy of the audited ProfitandLossStatementsforeachofthelast3financialyears) (Annexure-3)		
5.	Declaration for not being black-listed (Annexure – 4)		
6.	Formats for Technical bid (Section I)		
7.	NIT Declaration (Annexure – 7)		
8.	CertifiedcopiesofvalidPANdocument/CMMI-Level3orabove certification/ ISO 27001 Certification/GSTregistration		
9.	Technical Capability / Past Projects (Annexure – 8)		
10.	Bidder's Understanding of the Project requirements		
11.	Technical Solution Proposed		
12.	Approach and Methodology		
13.	Compliance to Scope of Work		
14.	Certificate from HR department mentioning the relevant manpower strength.		

15. Formats for Technical Bid

Annexure 7- NIT Declaration

(To be submitted on the letterhead of the bidder)

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Ref: Tender No. XXX

Sub: Submission of proposal in response to RFP for Engagement of System Integrator (SI)/OEM's for procurement ICT Hardware including Installation, Configuration, Commissioning for enablement of ERP Solution at Assam Gas Company Limited (AGCL)

Having examined the Bid Documents and the Terms of Reference including all attachments thereto, all addenda, all corrigenda, the receipt of which is hereby duly acknowledged, we the undersigned offer to perform the services in conformity with the said conditions of Contract and Terms of Reference for the quoted sum as indicated in the Priced Bid (BoQ) submitted online.

We undertake, if our Bid is accepted, to commence the work within (_) days calculated from the date of issue of Letter ofAward (LoA).

If our Bid is accepted, we will obtain the guarantee of a bank in a sum not exceeding _____for the due performance of theContract.

We agree to abide by this Bid for a period of 180 days from the date fixed for Bid closing and it shall remain binding upon us and may be accepted at any time before the expiration of thatperiod.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof in your notification of award shall constitute a binding Contract between us.

We understand that you are not bound to accept the lowest or any Bid you may receive.

Datedthis_____dayof_____2021.

Authorized Person'sSignature: _____
Name:_____
Designation: _____
Seal of the Bidder:

Annexure 8- Technical Capability/Past Projects

General Instructions on Preparation of the Technical Proposal

Bidders have to submit a very structured and organized technical bid, which will a critical component and will be analyzed by Technical Evaluation Committee for different compliances with regards to the requirements of the project.

The document submitted must be searchable and well indexed without any handwritten material. Quality and completeness of the information submitted by the Bidder will matter a lot for carrying out fair evaluation of the bidder's capability.

The experience in several projects is to be submitted in the format mentioned below:

#	Criteria	Details
	Client Information	
1	Name of the Client	
2	Name of the person who can be referred to from Clients' side, with name, designation, postal address, contact phone, fax number, email id)	
3	Nature of Business / operation of Client	
	Project Details	
4	Brief description of the Project	
5	Date of Contract Award	
6	Date of Datacenter/ICT Project Go-Live Date	
7	Brief scope of Project and Business Requirement	
8	Project Location	
9	Work Order value	
	Supporting Documents	
10	Copies of Work Order issued by the Customer detailing scope of work and values of project incl. taxes	
11	Work completion certificate by the Customer	

Signature with Official Stamp:

Name of Authorized Signatory:

Designation:

Annexure 9- Undertaking of Total Responsibility

Date:

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Ref:

Sub: Self-certificate regardingTotal Responsibility

Dear Sir,

This is to certify that we undertake total responsibility for the successful and defect free installation and commissioning of the proposed ICT infrastructure solution, as per the requirements of the RFP. In addition, we shall undertake and rectify all defects to ensure system performance within the warranty period as per the terms of this RFP.

Thanking you,

Yours faithfully

(Signature of the Authorized signatory of the Bidding Organization)

Name:

Designation:

Date:

Time:

Seal:

Business Address:

Annexure 10- Schedule of Delivery

The Data Center Implementation project at AGCL is expected to be completed within 5 months of initiation date of the project. The Bidder is expected to furnish the details of the milestone dates as per below format in line with AGCL's implementation plan as mentioned in Section- "Project Timeline and Payment Schedule".

Sl. No.	Activity Title	Schedule Date of Start of Activity	Schedule Date o Completion of Activity
1.			
2.			
3.			
4.			
5			
6.			
7.			
8			
9.			
10.			

Signature:
Name of Authorized Signatory:
Designation:

Annexure 11- Resource Deployment

Format: Month-wise Resource Deployment Plan

Bidder should provide a breakup of hours per month and per project phase for each of the role that will be deployed for ICT infrastructure deployment.

Sl. No.	Role	<Project Phase>				Total
		Month 1	Month 2	…	Month n	
1	Project Manager	<No. of Hours>	<No. of Hours>		<No. of Hours>	
2	ICT Architect					
3	ICT Engineer					
4	Any Other					
5	……					

Signature:
Name:
Designation:
Date:
Business Address:
Seal:

Annexure 12- Format of CV for Proposed Professional Staff

#	Description	To be filled by the bidder for each resource
1.	Name of the person	
2.	Role in the Project	*As per Technical Evaluation Criteria – Competency of Key Personnel Proposed*
3.	Educational Qualification	*<Photocopies of certificates to be provided>*
4.	Total number of years of experience	
5.	Number of years with the current company (the Bidder)	*<To be certified by the HR Dept. with employee ID>*
6.	Functional area / expertise	
7.	Certification	*<Photocopies of certificates to be provided>*
8.	Number of complete life cycle Datacenter implementations carried out (provide details)	
9.	The names of customers for which the person was a Project Manager/Technical/Domain consultant (Please provide the relevant names)	

Signature:
Name:
Designation:
Date:
Time:
Seal:
Business Address:

16. Bill of Quantity and Services

Annexure 13- Bill of Quantity

A. Prices are to be quoted in e-Tender portal only and not in physical bid. If it has been found that the bidder has mentioned the price anywhere in the physical tender, the bid will summarily be rejected.

B. The prices shall be quoted in Indian Rupees only. The parameter will be used to determine the successful bidder.

C. The price quoted should be exclusive of applicable taxes, duties, fees, levies, and other charges as may be applicable.

D. During the payment stage, AGCL reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated.

E. AGCL reserves the right to increase/decrease the line item and quantity at the time of placement of Letter of Intent/Purchase Order as mentioned in the BoQ.

Annexure 14- Performance Bank Guarantee

(On non-judicial stamp paper of appropriate value to be purchased in the name of executing Bank)

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Dear Sirs,

M/s have been awarded the work of for AGCL, DULIAJAN - Assam

The Contracts conditions provide that the CONTRACTOR shall pay a sum of (as full Contract Performance Guarantee in the form therein mentioned. The form of payment of Contract Performance Guarantee includes guarantee executed by Nationalized Bank, undertaking full responsibility to indemnify AGCL, in case of default.
The said has approached us and at their request and in consideration of the premises we having our office at have agreed to give such guarantee as hereinafter mentioned.

1. We hereby undertake and agree with you that if default shall be made by M/s in performing any of the terms and conditions of the tender or in payment of any money payable to AGCL, we shall on demand pay without any recourse to the contractor to you in such manner as you may direct the said amount of Rupees XXXXXXXXXXXXXX only or such portion thereof not exceeding the said sum as you may from time to time require.
2. You will have the full liberty without reference to us and without affecting this guarantee, postpone for any time or from time to time the exercise of any of the powers and rights conferred on you under the contract with the said and to enforce or to forbear from endorsing any powers or rights or by reason of time being given to the saidwhich under law relating to the sureties would but for provision have the effect of releasing us.
3. Your right to recover the said sum offrom us in manner aforesaid will not be affected or suspended by reason of the fact that any dispute or disputes have been raised by the said M/s.and/or that any dispute or disputes are pending before any officer, tribunal or court.
4. The guarantee herein contained shall not be determined or affected by the liquidation or winding up dissolution or changes of constitution or insolvency of the said but shall in all respects and for all purposes be binding and operative until payment of all money due to you in respect of such liabilities is paid.
5. This guarantee shall be irrevocable and shall remain valid up to . If any further extension of this guarantee is required, the same shall be extended to such required period on receiving

instruction from M/sbehalf this guarantee is issued.
on whose

6. The Bank Guarantee's payment of an amount is payable on demand and in any case within 48 hours of the presentation of the letter of invocation of Bank Guarantee. Should the banker fail to release payment on demand, a penal interest of 18% per annum shall become payable immediately and any dispute arising out of or in relation to the said Bank Guarantee shall be subject to the jurisdiction of DIBRUGARH Courts.

7. We have power to issue this guarantee in your favour under Memorandum and Articles of Association and the undersigned has full power to do under the Power of Attorney dated granted to him by the Bank.

WITNESS: SIGNATURE

NAME:

Designation:

SIGNATURE:

NAME:

Designation:

Bank Stamp

Date:

Bidders must indicate the full postal address of the bank along with the bank's E-mail / Fax from where the BG is issued

Annexure 15- Statement of No Deviation

To be submitted on Bidder's Letterhead

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

There are no technical deviations (null deviations) from the requirement specifications of tendered items and schedule of requirements. The entire work shall be performed as per your specifications and documents.

This is to certify that our proposed solution meets all the requirements of the RfP including but not limited to Scope of Work, stated Project Outcomes (including SLAs), Business Requirements and Functional Specifications/ Requirements.

We further certify that our proposed solution is equivalent or better than the minimum technical specifications as given in the RFP.

In case, any item of hardware or software is found non-compliant at any stage during project implementation, it would be replaced with a fully compliant product/solution at no additional cost to AGCL. In case of non-adherence of this activity, AGCL reserves the right to cancel the contract, in case the said Contract is awarded to us by AGCL.

We further confirm that our commercial proposal is for the entire scope of work, comprising all required components and our obligations, for meeting the scope of work.

Authorized Person'sSignature: _____

Name:_____

Designation:_____

Date:

Seal of the Bidder:

NOTE: Assam Gas Company Ltd expects the bidders to fully accept the terms and conditions of the bid document. However, should the bidders still envisage some exceptions/deviations to the terms and conditions of the bid document, the same should be indicated as per above format and submit along with their bids. If the "Statement of Compliance" in the above Proforma is left blank (or not submitted along with the technical bid), then it would be construed that the bidder has not taken any exception/deviation to the tenderrequirements.

Annexure 16- Warranty Support by OEM/ Bidder

To be submitted on Bidder's Letterhead

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

The OEM/Bidder for all theequipment's which are a part of this RFP should be able to support the Warranty andReplacement services efficiently.

Note: Bidder to provide supporting credentials from respective OEM's in their letter heads supporting the below statement.

We the bidder on behalf of OEM's hereby confirm that we will be able to support the warranty for the equipment efficiently as per the conditions of this RFP for period defined.

Additionally, we warrant that the equipment(s) supplied under the contract would be newly manufactured, free from all encumbrances, defects and faults in material or workmanship or manufacture, shall be of the highest grade and quality, shall be consistent with the established and generally accepted standards for materials of the type ordered, shall be in full conformity with the specifications, drawings of samples, if any, and shall operate as designed. We shall be fully responsible for its efficient and effective operation. We also warrant that the services provided under the contract shall be as per the Service Level Agreement (SLA) with AGCL.

The obligations under the warranty expressed above shall include all costs relating to labour, spares, maintenance (preventive as well as unscheduled), and transport charges from site to manufacturer's works / service facilities and back for repair or modification or replacement at site of the equipment or any part of the equipment, which under normal care and proper use and maintenance proves defective in design, material or workmanship or fails to operate effectively and efficiently or conform to the specifications and for which notice is promptly given by AGCL to us (Bidder). We shall provide on-site support for all the equipment and services supplied hereunder during the period of this warranty (5 years after acceptance for equipment or Go-Live whichever is later).

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:
Place:
Designation:
Date:

Annexure 17- Service Level Compliance

To be submitted on Bidder's Letterhead

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Sub: Undertaking on Service Level Compliance

Dear Sir/Madam,

I/We as Implementing Agency do hereby undertake that we shall monitor, maintain, and comply with the service levels stated in the RFP to provide quality service to AGCL.

However, if the proposed resources,are found to be insufficient in meeting the RFP and/or the service level requirements given by AGCL, then we will augment the same without any additional cost to AGCL.

Yours sincerely,

(Seal & Signature of the Authorized signatory of the System Integrator)

Name:

Place:

Designation:

Date:

17. Pre-Qualification Annexures

Annexure 18- Non-Termination Declaration

Certificate for Any Direct Contract Agreement of ICT Infrastructure with AGCL not having been terminated in last five (5) years

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Sub: -Setting up of Datacenter at AGCL.

Dear Sir,

Certificate

I / We ..... hereby confirm that any Contract awarded directly or as a partner to a consortium or JV, with AGCL has not been terminated in last five (5) years from date of issue of RFP.

Yours faithfully,

Signature & Seal of the Authorized Signatory

Name and Designation

Date:- Place:-

Annexure 19- Human Capital Strength

Human Capital Strength - Resource Strength of the Bidder

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Sub: -Setting up of Datacenter at AGCL

Dear Sir,

Certificate from Bidder's HR Department for minimum number of full-time resources on the payroll of the company, as required in the RFP of_____

I, _____certify that I am_____of M/s (Name of the Bidder) under the laws of and that we have (number) of full-time technically qualified ICT infrastructure professionals on our payroll for providing technical services related to supply, installation, testing & commissioning followed by operation & maintenance of Data Center ICT Infrastructure, other ICT Infrastructure and associated packaged software, etc., out of which (number) employees have minimum three (3) years of experience of working in Data Center environment and have experience of successful implementation, operation & maintenance of Data Center ICT infrastructure including Servers, Storage, Backup Solution, Data Center Networking, etc.

It is further to certify that we have ___X no.____(number) of OEM certified professionals on our payroll having valid certifications from OEMs which are relevant to the platform, product & technology proposed for offered solution and for which the resource has been proposed in the bid submitted by us/ {M/s (Nameof the Bidder). (Please provide breakup/details as per availability)

Yours faithfully,

Signature & Seal of the Authorized Signatory
Name and Designation
Date:- Place:-

I / We .....(Name of the Bidder) hereby confirmthat above HR Personnel is duly authorized to sign the Certificate for and on behalf of the HR Department of Bidder.

Signature & Seal of the Authorized Signatory of bidder
Name and Designation
Date:- Place:-

Annexure 20- Self Certification- Cyber/Information Security Threat

Self-Certificate for not being Under Declaration of Ineligibility for any Cyber or Information Security Threat by any Sovereign Government.

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Sub: - Setting up of Datacenter at AGCL.

Dear Sir,

I / We ..... hereby confirm that neither our firm nor any of our offered products under this bid has/have been under declaration of ineligibility for any cyber or information security threat by any Sovereign Government.

Yours faithfully,

Name

In the capacity of:

Signature & Seal

Duly authorized to sign the Authorization for and on behalf of the OEM in India

M/s
Counter Signature & Seal of the AuthorizedSignatory
Name andDesignation
Date & Place

Name & Address of Firm/Company (Bidder):

This self-certificate/form should also be signed by an authorized person of OEM in India who is the competent authority and having the power of attorney to sign & issue the required certificate/declaration. The bidder should include the aforesaid power of attorney of the authorized person of the OEM in India in its bid.

Annexure 19- Compliance Statement in accordance with the BOQ & RFP

To

Managing Director
Assam Gas Company Limited (AGCL),
Duliajan,Dibrugarh
Assam, 786602

Sub: - Compliance statement of the products quoted

Dear Sir,

The compliance statement of the product as per data sheet is as follows:

Sl. No	Name of the Product	Technical specification as RFP/BoQ	Compliance reference as per Data sheet
1.			
2.			

Signature & Seal of the Authorized Signatory
Name and Designation
Date:- Place:-