United Nations
Educational, Scientific and
Cultural Organization

क्षेत्रीय जैव प्रौद्योगिकी केन्द्र
Regional Centre
for Biotechnology

Regional Centre for Biotechnology

Notice Inviting e-Tender

for

"Supply, Installation, Testing, Commissioning (SITC)

of Indian Biological Data Centre (IBDC)

at NIC Bhubaneswar Data Centre and RCB, Faridabad

on Turnkey Basis and its Day to-day operations"

Regional Centre for Biotechnology
NCR Biotech Science Cluster
3rd Milestone, Faridabad-Gurugram Expressway
Faridabad - 121 001
Phone: 91 129 2848800

INDEX

REGIONAL CENTRE FOR BIOTECHNOLOGY

An institution of education, training & research

(Established by the Dept .of Biotechnology, Govt .of India under the auspices of UNESCO)

NCR Biotech Science Cluster, 3rd Milestone, Faridabad-Gurugram Expressway, Faridabad

Tender No.- RCB/NIT/08/20-21/IBDC **Date: 24.12.2020**

1. TENDER NOTICE

Online tenders are invited on behalf of the Executive Director, RCB under Two-Bid System (Technical bid and Financial bid) from reputed System Integrator for the work: "Supply, Installation, Testing, AND Commissioning (SITC) of Indian Biological Data Centre (IBDC) at NIC, Bhubaneswar Data Centre and RCB, Faridabad on Turnkey Basis and Day to-day operations' of IBDC as per the schedule, specifications and as per the terms and conditions mentioned in this tender document. Note, "Neither off-line/physical bids shall be accepted nor any such request will be entertained on any ground/reason".

NOTICE INVITING TENDER

Website Url :	https://rcb.res.in
Address	Regional Centre for Biotechnology, NCR Biotech Science Cluster 3rd Milestone, Faridabad - Gurugram Expressway Faridabad - 121001, Haryana.
Contact Details	Executive Director, RCB, Phone: 0129-2848800
Name of Work	Supply, Installation, Testing, AND Commissioning (SITC) of HPC and storage setup for Indian Biological Data Center (IBDC) at NIC Bhubaneswar Data Center and RCB, Faridabad on Turnkey Basis and Day to-day operations of IBDC.
Earnest Money	**Rs. 90 Lakh** (Rupees Ninety Lakh only) to be deposited Online through e-tender portal.
Date of Pre-Bid Meeting	31.08.2020 at 11:00 Hrs (online mode)
Tender Processing fees	To be deposited online through e-tender portal.
Tender Closing Date & Time	22.02.2021; 15:00 Hrs (extended date)
Date of Opening of Technical bid	22.02.2021; 15:30 Hrs (extended date)
Date of Opening of Financial bid	To be declared later

2. PRE QUALIFICATION CRITERIA

2.1 The bidder must be a Goods Service Tax (GST) registered firm or company.

2.2 The bidder should have completed,

2.2.1. At least one similar work of value not less than **Rupees 3600.00 Lakhs (In INR)** in the last seven years OR

2.2.2. Two similar works each of value not less than **Rupees 2250.00 Lakhs (In INR)** in the last seven years OR

2.2.3. Three similar works each of value not less than **Rupees.1800.00 Lakhs (In INR)** in the last seven years ending on previous day of last day of submission of tender.

Note: Similar work means **Supply, Installation, Testing, and Commissioning (SITC)** of HPC and storage servers of similar capacity in any other Govt. Department/Defence organization/PSU, university, Biotech company, Research institution or reputed private sector company during last FIVE (05) years. The completed works will be open to inspection and in case works is not up to the standard, the tender will summarily be rejected & no queries will be entertained in this regard. Please refer to "ANNEXURE-XI" in this regard. Self-attested copies of the completion certificates issued by Organization should be enclosed with the technical bid.

2.3 Average annual financial turnover should be at least **Rupees 1350.00 Lakhs (In INR)** during the immediate last three consecutive financial years. i.e. FY 2017-18, 2018-2019 and 2019-20.

2.4 The bidder shall have minimum solvency of **Rupees 1000.00 Lakhs (In INR)**. Solvency certificate from the Bidder's Banker should be submitted.

2.5 The server OEM should have minimum two entries in the supercomputer list (Jan-2020) maintained by CDAC (which can be downloaded at http://topsc.cdacb.in/) OR should have at least five installations listed in Top 500 supercomputers listed at http://www.top500.org (Nov-2019).

2.6 The OEMs (OEMs of Servers, Storages, Backup Solution and all other materials/items) will be responsible for supply, installation, configuration, commissioning, testing, maintenance and support for both hardware and software during the warranty period. Details of the engineers (Emp Id No., years of experience within organization & copy of the emp. Id Card) to be shared with RCB before the installations starts.

2.7 The OEMs (OEMs of Servers, Storages, Backup Solution and all other materials/items) should have a registered office in India, which should have registered at least one year before the tender submission date. Bidder has to submit documentary evidence to prove the same.

2.8 Any bidder from a country which shares a land border with India will be eligible to bid only if the bidder is registered with the Competent Authority and the bidder should be in compliance with the F. No. 6/18/2019-PPD dated 23rd July 2020 of Department of Expenditure, Ministry of Finance, Government of India and certificate to be submitted as per **ANNEXURE-XVII** (Certificate for tender).

2.9 The OEMs (OEMs of Servers, Storages, Backup Solution and all other materials/items) must have spare inventory depot in India for quick after sales support to the Centre.

Bidder has to submit declaration with address proof for the same.

2.10 The Bidder can be OEM or their authorized Dealer /business partner.

2.11 In case the bidder is not OEM, bidder must submit letter from OEM stating that OEM is responsible to provide warranty and support in case the bidder is not able to support or resolve the technical issues during the installation and warranty period. This condition applies to all major components like all IT equipment's (OEM or Manufacturer should be ISO 9001: 2000/18000:1, ISO 14001, ISO/IEC 27001:2013 and ISO 45001 certified. i.e. server, storage etc.), and electrical items like UPS and Cooling systems.

Note: Bidder should submit a certificate from OEM of data centre cooling equipment / heat exchangers that all cooling components quoted conform to their standards and specifications.

2.12 Bidder should submit the Manufacturer's Authorization Form (MAF) for the quoted products i.e. IT h/w, UPS, Cooling System, Racks etc.

2.13 A copy of the authorization by the Proprietor / Partners / Director(s) or by all the partners of the Agency (as the case may be) in case the Bid documents are signed & sealed by an authorized person.

2.14 The firm should have not been blacklisted, debarred, declared non-performer or expelled from any work of Union Government/State Governments/ PSUs etc. during the last 5 years. They should also submit a self-declaration on its letterhead for the same.

2.15 It is considered necessary that the Tenderer should visit both the sites (NIC, Bhubaneshwar and RCB, Faridabad) and get clear idea about the work involved, before quoting. Tenderer(s) should study all the particulars of both the sites and the nature of the work. Attending/participating in the pre Bid meeting at RCB Faridabad by the bidders is mandatory. The bidders will not be allowed to participate in the pre-bid meeting if the site inspections certificate are not presented. Refer "ANNEXURE-XIII".

2.16 All documents should be page numbered, stamp and signed by the authorized signatory.

2.17 Bidder should submit a document endorsing that the quoted components / items are new, latest and not nearing end of life or end of support from OEM in next 5 years applicable from the date of acceptance.

2.18 A prospective bidder who requires clarification regarding the contents of the bidding documents can clarify during pre-bid meeting. During evaluation and comparison of bids, the Centre may, at its discretion, ask the bidder for clarification of his bid. The request for clarification will be given in writing and no change in prices or substance of the bid will be sought, offered or permitted. No post-bid clarification on the initiative of the bidder will be entertained.

2.19 No bid shall be modified after the deadline for submission of bids. No bid may be withdrawn in the interval between the deadline for submission of bids and expiration of the period of bid validity specified. Withdrawal of a bid during this period will result in Bidder's forfeiture of bid security. A withdrawal notice may be sent by fax/email but it should be followed by a signed confirmation copy which may be sent by hand/post and such signed confirmation should reach the Purchaser not later than the deadline for

submission of bids.

2.20 Proposed architecture should be tested and verified by the OEM and proof for the same to be submitted on OEM letterhead. The testing should also prove that architecture (combination of Server/storage/network) is designed to get best-optimized performance, deployment to be made quickly and have minimum overheads.

NOTE: The contractor shall clearly indicate their legal constitution and the person signing the bid shall state his capacity and also source of his ability to bind the Contractor. The power of attorney or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the contractor, shall also be submitted along with the tender. The Centre may reject outright any bid not supported by adequate proof of the signatory's authority.

3. REGISTRATION PROCESS

3.1 Bidders to enrol on the e-Procurement module of the portal https://dbt.euniwizarde.com by clicking on the link "Bidder Enrolment". Enrolment on the e-wizard Portal is free of charge.

3.2 The bidders to choose a unique username and assign a password for their accounts. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the e-Wizard Portal.

3.3 Bidders to register upon enrolment their valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India with their profile.

3.4 Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSCs to others, which may lead to misuse. Foreign bidders are advised to refer "DSC details for Foreign Bidders" for Digital Signature requirements on the portal.

3.5 Bidder then logs in to the site through the secured login by entering their user ID / password and the password of the DSC / e-Token.

4. TENDER DOCUMENTS SEARCH

4.1 Various built in options are available in the e-Wizard Portal, which is further synchronizing with CPP Portal to facilitate bidders to search active tenders by several parameters. These parameters include Tender ID, organization, location, date, value, etc.

4.2 There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as organization name, form of contract, location, date, other keywords etc. to search for a tender published on the Online Portal.

4.3 Once the bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective 'My Tenders' folder. This would enable the Online Portal to intimate the bidders through SMS / e- mail in case there is any corrigendum issued to the tender document.

4.4 The bidder should make a note of the unique Tender ID assigned to each tender, in case

they want to obtain any clarification / help from the Helpdesk of the e-Wizard portal.

5. BID PREPARATION

5.1 Bidder should take into account any corrigendum published on the tender document before submitting their bids.

5.2 Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.

5.3 Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid.

5.4 Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / RAR / DWF formats. Bid documents may be scanned at least 100 dpi with black and white option and the scanned documents should be legible. Illegible bids will not be considered.

5.5 Copy of constitution or legal status of the bidder manufacturer / Sole proprietorship / firm / agency etc.

5.6 Experience Certificates in line with the pre-qualification criteria mentioned in the tender document.

5.7 Copy of PAN Card / GST Registration.

5.8 Brochure, original technical catalogue with detailed specification and picture of the product offered, if relevant.

5.9 Earnest Money Deposit: The bidder will be required to deposit the Earnest Money Deposit (EMD) for an amount of **Rupees Ninety (90) Lakh (In INR)** through online portal**.**

5.10 EMD Fee are exempted for MSME/ NSIC vendors etc. however tender processing fee has to be paid by all the vendors as this fee is being charged by the Online Portal service provider directly.

5.11 The bidder should must have their registered office/ branch/ service Centre in Delhi-NCR.

6. BID SUBMISSION

6.1 Bidder to log into the site well in advance for bid submission so that he/she upload the bid in time i.e. on or before the bid submission deadline. Bidder will be responsible for any delay due to other issues.

6.2 The bidder to digitally sign and upload the required bid documents one by one as indicated in the tender document.

6.3 Bidder to select the payment option as “Online” to pay the tender fee/ EMD wherever applicable and enter details of the instrument.

6.4 A standard Bo format (preformat of price bid) has been provided with the tender document to be filled by all the bidders. Bidders to note that they should necessarily submit their financial bids in the prescribed format and no other format is acceptable.

6.5 The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.

6.6 All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data, which cannot be viewed by unauthorized persons until the time of bid opening.

6.7 The uploaded tender documents become readable only after the tender opening by the authorized bid openers.

6.8 Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. along with the date & time of submission of the bid with all other relevant details.

6.9 Kindly add scanned PDF of all relevant documents in a single PDF file of compliance sheet.

7. ASSISTANCE TO BIDDERS

7.1 Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.

7.2 Any queries relating to the process of online bid submission or queries relating to e-Wizard Portal in general may be directed to the 24x7 e-Wizard Helpdesk. The contact numbers for the helpdesk are 011-49606060, 011-23710092, 011-23710091, +91-9355030602.

8. TERM AND CONDITIONS

8.1 Standard General Conditions of the Contract (GCC) form 7/8 (modified and corrected up to date) of CPWD shall be followed except otherwise stated elsewhere in the tender document.

8.2 **Completion period of work:** Twenty Two (22) Weeks from date of issue of work order.

8.3 **Validity of the bids:** The bids should be valid for a period of 180 days from the receipt of technical bid. This has to be so specified by the tenderer in the commercial bid.

8.4 **Warranty / Guarantee:** Bidder must provide three (03) year comprehensive on-site warranty inclusive of two (02) year additional comprehensive onsite warranty against the defect of any manufacturing and workmanship. The warranty period will commence from the date of the satisfactory installation / commissioning/handing over of goods. No offer of the vendor will be accepted without warranty/ guarantee of their supplied/ installed goods.

8.4.1. The bidder shall provide three (03) year comprehensive on-site warranty plus two

(02) year additional warranty with 24 X 7 operational support with four hours of response time for any hardware related issue/problem for the IBDC and its equipment/material under the contract and warranty that the equipment supplied conform to technical specifications prescribed in this tender document and shall perform according to the said technical specifications.

8.4.2. OEM Certified manpower support (as per SLA) must be having at least 5 years' experience for handling similar/large IT infrastructure needs to be provided by the contractor/ bidder during the warranty period. Relevant experience certificates must be deposited to the Centre.

8.4.3. Additional 2 years' warranty and support cost will be considered while identifying the L1 vendor, but order for the same will be issued at the end of third year.

8.4.4. The Institute will have the right to negotiate the price quoted by the successful bidder for additional 2 years' comprehensive onsite warranty.

8.4.5. If within the period of warranty, the goods are reported by the Centre to have failed to perform as per the specifications, the bidder / contractor shall either replace or rectify the same free of charge, within a maximum period as per SLA of notification of such defect received by the contractor, provided that the goods are used and maintained by the Centre as per instructions contained in the Operating Manual. Warranty of the Data Centre equipment would be extended by such duration of downtime. Record of the down time would be maintained by the user in the online logbook / complaint management system. Spares required for warranty repairs shall be provided free of cost by the contractor. The Seller also undertakes to diagnose, test, adjust, calibrate and repair /replace the goods/tool arising due to accidents by neglect or misuse by the operator or damage due to transportation of the goods during the warranty period, at the cost mutually agreed to between the Centre and the contractor /bidder.

8.4.6. The warranty should also cover all the consumable spares including batteries.

8.4.7. The bidder / contractor shall associate technical personnel of the Maintenance agency and Quality Assurance Agency of the Centre during warranty repair and shall also provide the details of complete defects, reasons and remedial actions for defects into online query management system.

8.4.8. If equipment fails frequently and/ or, the cumulative down time exceeds 5% of the warranty period, the complete equipment/material shall be replaced free of cost by the bidder / contractor within a stipulated period of 05 days of receipt of the notification from the Centre. Warranty of the replaced equipment / material would start from the date of acceptance after Joint Inspection by the Centre and bidder / contractor or the date of installation and commissioning.

8.4.9. During the warranty period, the Seller shall carry out all necessary servicing / repairs / up-gradation of software applications to the equipment under warranty at the current location of the equipment. Prior permission of the Centre would be required in case certain components/sub systems are to be shifted out of location. On such occasions, before handing over the goods or components, valuing more than Rupees One Lakh, a suitable bank guarantee is to be obtained from the firm to safeguard the purchaser's interest.

8.5 The details of the proposed layout architecture at the two sites should be provided with the technical bid.

8.6 The Tenderer may furnish any additional information, which he thinks is necessary to establish his capabilities to successfully complete the envisaged work. He is however, advised not to furnish superfluous information. No information shall be entertained after submission of tender documents unless it is called for by the RCB.

8.7 Any information furnished by the tenderer either found to be incorrect immediately or later, would render him liable to be debarred from tendering/taking up of work in RCB.

8.8 Any variation in the terms and conditions of the general/special conditions for payment, tender fees, security deposit, etc. is not acceptable to RCB and such tenders will be rejected straight away.

8.9 RCB reserves the right to award the contract in full or in part as per the decision of the competent authority

8.10 RCB is not responsible for any delay in receipt of the application / receipt of tender documents etc. It is the responsibility of tenderer to make sure that the tender is uploaded in time.

8.11 Acceptance of tender shall rest with the RCB, which shall not be bound to accept the lowest tender and reserves to itself the right to reject any or all tenders received without assigning any reasons therefor.

8.12 **Installation**: all the works shall be completed within Twenty Two (22) weeks from the date of issue of work order by the Centre. All the aspects of safe installation shall be the exclusive responsibility of the supplier. If the supplier fails to complete the work on or before the stipulated date, then a compensation for delay of work @ 1.5% per month of Tendered Value of work of delay of work to be computed on per day basis provided always that the total amount of compensation for delay to be paid under this Condition shall not exceed 10% of the Tendered Value of work.

8.13 **Country of Origin:** All goods and services to be supplied and provided under the contract shall have the origin in India or in the countries with which the Government of India has friendly trade relations. The word "origin" incorporated in this clause means the place from where the goods are manufactured or from where the services are arranged.

9. PAYMENT TERMS

The payment shall be made in the bank account of the bidder / contractor directly through e-payment mode. It is mandatory for the Bidders to provide their bank account numbers and other relevant details for payment so that payments could be made through ECS/NEFT/RTGS mechanism instead of payment through Cheque. The pre-receipted paste of 1 revenue stamp on each bill in triplicate may be send to this office for payment after satisfactorily delivery & Installation of the goods. The bill should have full particulars of the items. Detailed schedule of payment is as under:

9.1 The Performance Security Deposit amounts to 5% of tender value (exclusive of 2 years' additional warranty) and must be deposited by successful bidder within 15 days of award of work in the form of Online/Demand Draft/Bank Guarantee/ FDR, from

Nationalized/scheduled bank valid up to 3 Months from issue of work order, drawn in favour of "Executive Director, Regional Centre for Biotechnology", Payable at Faridabad. Performance Security should remain valid for a period of sixty days beyond the date of completion of all contractual obligations of the supplier including warranty obligations.

9.2 The Security Deposit at the rate of 5% will be collected by deductions from each running bills as well as final bill of the bidder / contractor at the rates mentioned and it will be released after 12 months from the date of overall completion of work and basis of satisfactory / acceptance report issued by the client.

9.3 Payment of the balance of the value of the supplies may be payable after completion of the defect liability period and as reduced by any deductibles and/or the amount liveable towards liquidated damages, if any.

9.4 The PAYMENT will be released in the following stages:

9.4.1. 60% payment (only for hardware) will be made after complete delivery of the equipment's in good condition and acceptance as may be payable and as reduced by any deductibles and/or the amount liveable towards liquidated damages, if any plus 100% taxes, duties etc. as applicable on production of proof of inspection, receipt and acceptance at RCB between 15 to 20 days.

9.4.2. Other Pending payment of the total work value will be released after completion of project, commissioning, testing, training, and submission of license keys, warranty certificate, satisfactory reports etc.

9.4.3. Payment will be released within 30 days of receipt of bill/invoice subject to successful installation and user acceptance.

9.5 No payment will be made for goods rejected

9.6 Security Deposit will be released after successful expiry of Defect Liability Period (12 months) which will commence from date of completion.

9.7 EMD can be adjusted (released) against Performance Security Deposit.

9.8 The above rates must be inclusive of all applicable Taxes, handling and freight charges etc. & all applicable taxes shall be deducted at source from the passed amount of the contractor bill.

9.9 The potential bidder has to visit both the sites at their own cost and submit a detailed site survey report for the consideration of the Competent Authority of RCB.

9.10 Taxes and Duties:

9.10.1. Price quoted should be inclusive of the taxes / duties. The applicable taxes should be mentioned in the relevant column provided for the purpose. In case space provided for the Tax remain blank, it will be presumed that either no tax is payable or prices are inclusive of all taxes. RCB is a Public Funded Research Institution and registered with the Department of Scientific and Industrial Research (DSIR).

9.10.2. If a Bidder is exempted from payment of any duty/tax up to any value of services from them, he should clearly state that no such duty /tax will be charged by him up

to the limit of exemption which he may have. If any concession is available in regard to rate/quantum of any Duty/ tax, it should be brought out clearly. Stipulations like, the said duty /tax was presently not applicable but the same will be charged if it becomes liveable later on, will not be accepted unless in such cases it is clearly stated by a Bidder that such duty/tax will not be charged by him even if the same becomes applicable later on. In respect of the Bidders, who fail to comply with this requirement, their quoted prices shall be loaded with the quantum of such duty /tax which is normally applicable on the item in question for the purpose of comparing their prices with other Bidders.

9.10.3. Any change in any duty/tax upward/downward as a result of any statutory variation taking place within contract terms shall be allowed to the extent of actual quantum of such duty/tax paid by the vendor. Similarly, in case of downward revision in any duty/tax, the actual quantum of reduction of such duty/tax shall be extended to the Centre by the bidder. All such adjustments shall include all reliefs, exemptions, rebates, concession etc. if any obtained by the bidder.

9.10.4. In case any new tax or levy or cess is imposed by Statute, after the last date stipulated for the receipt of tender including extensions (if any), the seller shall inform the Centre in writing within 15 days of imposition/Notification of said tax and thereupon necessarily and properly pays such taxes/ levies/ cess, The seller shall be reimbursed the amount so paid, provided such payments, if any, is not, in the opinion of the competent authority (whose decision shall be final and binding on the bidder / contractor) attributable to delay in execution of work within the control of the seller. The seller shall keep necessary books of accounts and other documents for the purpose of this condition as may be necessary and shall allow inspection of the same by a duly authorized representative of the Government and shall also furnish such other information/ document as may require from time to time.

9.11 **Risk & Expense clause:**

9.11.1. If the work or any part thereof not be established within the time or times specified in the contract documents, or if poor / substandard items / components / material are provided, the Centre shall after granting the contractor 05 days to cure the breach, be at liberty, without prejudice to the right to recover liquidated damages as a remedy for breach of contract, to declare the contract as cancelled either wholly or to the extent of such default.

9.11.2. If the Data Centre not established in accordance with the specifications / parameters by the contractor during the contract period the Centre shall be at liberty, without prejudice to the right to recover liquidated damages as a remedy for breach of contract, to declare the contract as wholly cancelled for breach of contract, or to the extent of such default.

9.11.3. Any excess of the contract price, services procured from any other service provider as the case may be, over and above the contract price, price appropriate to such default or balance/ difference shall be recoverable from the contractor. Such recoveries shall however, not exceed 10% of the values of the total contract."

10.CONTRACT DOCUMENT

10.1 The terms 'Contract document' means the Notice Inviting Tender, Tender form, Instructions to bidders, Special Conditions, General Conditions of Contract, Specifications, Price Schedule and Drawings and Articles of Agreement.

10.2 "RCB" shall mean Regional Centre for Biotechnology with its present office at 3rd milestone Faridabad - Gurugram Expressway, Faridabad 121001, Haryana.

10.3 The Contractor shall mean the sole proprietor, or firm or company whether incorporated or not, undertaking the works and shall include the legal representative or such individual successors, theirs, administrators or assignees of such sole proprietor, firm or company, as the case may be or the persons composing such firm or company of the successors of such firm or company and the permitted assignees of such individual or firms or company.

10.4 Client shall mean the officer designated by the Executive Director, RCB who shall supervise and shall be in charge of the work, and issue necessary instructions at site, on behalf of RCB.

10.5 Contractor shall strictly confirm specification, price schedule, general and special terms & conditions, if any, other matter contained in the tender documents issued by the RCB.

10.6 Failure of the successful contractor to lodge the required performance guarantee shall constitute sufficient grounds for the annulment of the Award and forfeiture of the Bid Security, in which event the RCB may call for new bids.

10.7 In the event of breach of contract by the contractor, the performance guarantee will liable to be forfeited by RCB.

11.TIME AND EXTENSION FOR DELAY

If in the opinion of the Client, the works is delayed by:

11.1 Force majeure.

11.2 Reasons of civil commotion, location combination of workers on strike or lock-out affecting any of the building trades.

11.3 In consequence of the contractor for not having received in due time necessary instructions from the Client for which he shall have specifically applied in writing.

11.4 Reasons of Client instruction: The Client shall make a fair and reasonable extension of time for completion of the contract works. Then upon the happenings of any such event causing delay, the Contractor shall immediately give notice thereof in writing to the Project-in-charge but shall nevertheless use constantly his best endeavour's to prevent or make good the delay and shall do all that may be reasonably required to the satisfaction of the Client to proceed with the works.

11.5 Request for rescheduling of date of completion and extension of time, to be eligible for consideration, shall be made by the Contractor in writing immediately after the happenings of the event causing delay. The Contractor may also, if practicable, indicate in such a request

the period for which extension is desired. In such case, the Client may give a fair and reasonable extension of time and reschedule the completion date. Such extension shall be communicated to the Contractor by the Client in writing within 2 Weeks of the date of receipt of such a request. Non- application by the Contractor for extension of time shall not be a bar for giving a fair and reasonable extension by Client and this shall be binding on the Contractor.

12.COMPENSATION FOR DELAY

12.1 Time is the essence of the contract. The time allowed for the work shall be strictly followed. If the supplier fails to complete the work on or before the stipulated date, then a compensation for delay of work @ 1.5% per month of tender value of work to be computed on per day basis provided always that the total amount of compensation for delay to be paid under this Condition shall not exceed 10% of the Tendered Value of work. The decision of Client about the delay shall final and binding.

12.2 If the contractor after award of work fails to deliver any item / part of the work within the time period allowed, RCB reserves the right to remove that particular component from the scope of main contractor and get it done through some alternative resources at the cost of main contractor.

13.WORK OPEN INSPECTION

13.1 All works under or in course of execution or being executed in pursuance of the contract shall at all times be open to inspection and supervision by the Client and/or his authorized subordinates, and the Contractor shall at all times during the usual working hours, and at all other times at which reasonable notice of the intention of the Client or his subordinate to visit the works shall have been given to the contractor, either himself be present to receive order and instructions, or have a responsible agent duly accredited in writing, present for that purpose. Order given to the contractor's agent shall be considered to have the same force as if the same had been given to the Contractor himself.

13.2 All works shall be executed subject to the approval in all respect of the Client who shall be entitled to direct at what point or points and in what manner these are to be commenced, and carried out from time to time.

14.INSPECTION, TESTING AND QUALITY CONTROL

14.1 RCB and/or its nominated representative(s) will, inspect and/or test the work / material to confirm their conformity to the tender specification at no extra cost to the RCB. The Inspection Authority to be designated by the RCB shall specify what inspections and tests are required and where they are to be conducted. The RCB shall notify the contractor in writing in a timely manner of the identity of any representatives retained for these purpose. All work / material shall be tested as stipulated in the latest specification of, Govt. /institutes. Contractor shall assign one project manager under whose supervision the project will be implemented.

14.2 The inspections and tests may be conducted on the premises of the tenderer or its subcontractor(s) or at the point of on completion of delivery at respective locations and a delivery certificate will be issued. If conducted on the premises of the tenderer or its subcontractor(s), all reasonable facilities and assistance, including access to

drawings and production data shall be furnished to the Inspectors at no charge to the RCB.

14.3 The representative of Centre shall inspect or test the items, which fail to conform to the specifications. The RCB may reject such items and the tenderer shall replace the rejected items, at no cost to the RCB, within a stipulated time period.

14.4 The RCB's right to inspect, test and where necessary, reject the items after its arrival at the final destination shall in no way be limited or waived by reason of the items having previously been inspected, tested and passed by RCB or its representatives.

14.5 Nothing shall in any way release the tenderer from Warranty/Guaranty or other obligations under the contract.

14.6 The RCB shall be the final authority to reject full or any part of the item that is not conforming to the specifications and other terms & conditions.

14.7 No payment shall be made for rejected items. The contractor must remove rejected items within one weeks of the date of rejection at their own cost and replace immediately. In case these are not removed, these will be auctioned at the risk and responsibility of the contractor without any further notice.

14.8 Bidder shall provide a detailed document to Centre towards inspection and testing mentioning the approach, test cases etc.

14.9 On completion of IBDC erection, the bidder shall perform and demonstrate inspection results stipulated in the document that was submitted earlier to RCB, Faridabad. RCB shall arrange Competent Authority for a joint inspection of the installation for completeness and correctness of the work. Any defect pointed out during such inspection shall be promptly rectified by the Bidder / Contractor.

14.10 The installation shall be then commissioned and tested in presence of authorities of NIC Bhubaneshwar & RCB Faridabad. All rectification, repair or adjustment work found necessary during inspection, the bidder without any extra cost shall carry out testing, commissioning and trial run.

14.11 Bidder shall appoint an empanelled Agency to perform DC Audit and shall ensure certification of Tier-II/ & above.

15.PACKING AND MARKING

15.1 The packing of items to be supplied directly at site, should be strong and durable enough to withstand, without limitation, the entire journey during transit including trans-shipment (if any), rough handling, open storage etc. without any damage, deterioration etc. As and if necessary, the size, weights and volumes of the packing cases shall also take into consideration, the remoteness of the final destination of the supplied Items and availability or otherwise of transport and handling facilities at all points during transit up to final destination as per the contract.

15.2 The quality of packing, the manner of marking within & outside the packages and provision of accompanying documentation shall strictly comply with the requirements as per site condition. In case the packing requirements are amended due to issue of any amendment to the contract, the same shall also be taken care of by the tenderer accordingly.

15.3 **Packing Instructions:** The tenderer shall make separate packages for each consignee (in case there is more than one consignee mentioned in the work order) and mark each package on three sides with the following with indelible paint of proper quality:

a) Name of the Work and Tender no.
b) Contract number and date
c) Brief description of items including quantity
d) Packing list reference number
e) Country of origin of supplied items
f) Consignee's name and full address
g) Tenderer's name and address

16.GUARANTEE CLAUSE

16.1 The contractor shall guarantee that all the material and components supplied and installed by him shall be free from defects due to faulty, material or workmanship.

16.2 The charge and any shortcomings found in the materials as specified shall be removed at no extra cost. The contractor shall provide the necessary personnel and tools for fulfilling the above guarantee. Period of the guarantee shall be five years from the date of handing over the complete installations at both the sites. During this period any or all components found to be defective shall be replaced or repaired free of cost.

16.3 If the defects are not removed within a reasonable time, the RCB may arrange to do at the contractor's risk and cost, without prejudice to any other rights.

16.4 **After Sales Service:** It should be made available on 24*7 on yearly basis. Complaints should be attended promptly as per SLA document (ANNEXURE – XVI). The service should be provided directly by the tenderer/authorized agent only.

17.PRICE FALL CLAUSE

If at any time during the validity of the project, the tenderer supplies such equipment's/stores as are under this tender enquiry, to any other organization at a price lower than the price quoted under this contract, he shall forthwith reduce the price payable under this tender for the equipment's/ stores being supplied from the date of coming into force of such reduction, the price of equipment's/ stores shall stand correspondingly reduced. In case of increase in market prevailing prices of the materials if claimed by the supplier, no price escalation will be payable.

18.TERMINATION

18.1 Being a standing offer, the work can be terminated by RCB by serving one month's notice to party. However, all the orders placed before the date of serving of such notice will be valid and binding on both the parties.

18.2 Termination of work order. Not with standing anything elsewhere provided herein and in addition to any other right or remedy available to RCB under the work or otherwise including right of RCB to claim compensation for delay, RCB may, without prejudice to his right against contractor in respect of any delay, bad workmanship or otherwise or to any claims for damage in respect of any breaches of the contract and without prejudice to any rights or remedies under any of the provisions of this work or otherwise and whether

the date for completion has or has not elapsed by intimation in writing, absolutely determine and terminate the Contract.

18.3 Default or failure by the contractor in any of the under mentioned cases, including but not limited to the following shall be the basis of taking action under this clause of the contract.

i. Failure to execute the works or any of them in accordance with the contract.

ii. Disobedience of any order or instruction of the Site Engineer and /or Engineer-in-charge.

iii. Negligence in carrying out the work or carrying out of work found to be unsatisfactory by the Client.

iv. Abandonment of the works or any part thereof.

v. If the Contractor misconduct in any manner.

vi. Delay in execution of work, which in opinion of Client shall delay the completion of work beyond the stipulated date of completion.

vii. Distress, execution, or other legal process being levied on or upon any of the Contractors goods and /or assets.

viii. Death of Contractor (if an individual)

ix. If the Contractor of any person employed by him shall make or offer for any purpose connected with the contract any gift, gratuity, royalty, commission, gratification or other inducement (whether money or in any other form) to any employee or agent to RCB.

x. The decision of the Executive Director, RCB as to whether any of the events/ contingencies mentioned in aforesaid clauses entitling RCB to terminate the contract has occurred shall be final and binding upon the Contractor. The jobs left however by the Contractor shall be got done at his risk and cost through the other agencies and the Contract shall be determined accordingly.

19.FORCE MAJEURE

Should any force majeure circumstances arise, each of the contracting party shall be excused for the non-fulfilment or for the delayed fulfilment of any of its contractual obligations, if the affected party within 14 days of its occurrence informs in a written form the other party. Force majeure shall mean fires, floods, natural disasters or other acts such as war, turmoil, strikes, sabotage, explosions, and quarantine restriction beyond the control of either party. The right of the contractor to proceed with the work shall not be terminated because of any delay in the completion of the work due to unforeseeable causes beyond the control and without the fault or negligence of the contractor, including but not limited to acts of god, or of the public enemy, restraints of a sovereign state, floods, unusual severe weather conditions.

20.ARBITRATION

Any claim, dispute or difference arising out of or in connection with this agreement and which cannot be settled by mutual consultations, shall be referred to sole Arbitration or an Arbitrator to be appointed by the Competent Authority of the RCB. The award of the Arbitrator shall be

final and binding between the parties as per the terms and conditions of the Agreement to be executed on award of contract. The Arbitration proceedings shall be governed by the Arbitration and Conciliation Act, 1996 and amended thereof shall be conducted in Haryana.

21. CRITERIA FOR EVALUATION OF THE TECHNICAL AND FINANCIAL BID

This project includes Supply, Installation, Testing, and Commissioning (SITC) of Indian Biological Data Centre (IBDC) at NIC Bhubaneswar Data Centre and RCB, Faridabad on Turnkey Basis and its Day to-day operations. All offers should be submitted online in two-bid system: Technical and Price Bids, separately. The proposal must include layout architecture and bill of quantities (BOQ). Interested contractors should visit the sites for physical check and status of the sites condition. Technical evaluation should be done as per eligibility criteria. The guidelines for evaluation of Bids will be as follows:

21.1 The bidder will not be allowed to be participate during the pre-bid meeting if the site inspections certificate not presented.

21.2 Only those Bids will be evaluated which are found to be received by the stipulated date and time and fulfilling all the eligibility and qualifying requirements as mentioned in the tender document, both technically and commercially.

21.3 Rates quoted by the bidder in the price bid / format in figures and words shall be accurately filled in so that there shall not be any discrepancy in the rates written in figures and words. However, if a discrepancy is found, the rates which correspond with the amount worked out by the contractor shall unless otherwise proved be taken as correct.

21.4 if the amount of an item is not worked out by the contractor or it does not correspond with the rates written either in figures or in words, then the rates quoted by the contractor in words shall be taken as correct. Where the rates quoted by the contractor in figures and in words tally, but the amount is not worked out correctly, the rates quoted by the contractor will unless otherwise proved be taken as correct and not the amount.

21.5 Technical Evaluations of the Bids will be carried out by a duly constituted committee on the basis of Bid Documents submitted by the bidder as per Eligibility criteria and technical specification given in the tender document. The committee will examine the bids to determine whether they are complete in all respect, whether there are any computational errors, whether the documents are genuine and properly signed and whether the bids are generally in order. The committee shall determine the conformity of each bid w.r.t. the bidding documents. As regard to financial evaluation of the Bids, the Gross amount quoted by the bidder as per the Price Bid format or as described under the bid document will be carried out by the committee.

21.6 The Price Bids of only those Bidders will be opened whose Technical Bids would found compliant after the evaluation of eligible criteria.

21.7 A duly constituted team of RCB & NIC may visit the office / establishment /factory of the bidders / contractor for establishing their credibility & verification of submitted documents.

21.8 Conditional Tenders/Non-compliance of any of conditions, set in tender document shall render the bid to disqualification. Any deviation from the clauses hidden / intentional /unintentional shall be considered as contravention of the clauses of tender document.

21.9 However, RCB shall not be bound to accept the lowest or any other tender or to assign any reason for non- acceptance or rejection of a tender. RCB reserves the right to accept any tender in respect of the whole or any portion of the work specified in the tender paper.

21.10 Even though any bidder may satisfy the above requirements, he/she would be liable to disqualification if he/she has:

21.10.1. Made misleading or false representation or deliberately withheld information in the forms, statements and enclosures required in the eligibility criteria document.

21.10.2. Record of poor performance such as abandoning work, not properly completing the contract, or financial failures/ weaknesses etc.

21.11 The bid of any bidder who has not complied with one or more of the conditions will be summarily rejected.

22.SCOPE OF WORK

A. INTRODUCTION

A wealth of information, representing diverse areas in Life sciences such as healthcare, genomics, proteomics, metabolomics, microbiomes, protein structures, natural compounds, agriculture and population genetics, is being generated in India. The modern sciences have become data-intensive and data-dependent, often requiring integrative analysis. However, in the absence of any central data repository for national biotechnology data, both sharing, and data-dependent research are restricted. Indian researchers, like their international counterparts, disseminate the scientific findings by publishing the results of their work in scientific journals.

Currently, Indian researchers deposit their data in international databases as mandated by most scientific journals and the data is available to others after the publication of scientific articles. However, the underlying raw data is not available in most cases and the data for studies that are unpublished never are available to other Indian researchers. Additionally, there are a lot of sensitive human and biodiversity data that needs to be stored within the country. Therefore, India must develop the right infrastructure to store, manage, archive and distribute all biological data.

B. OBJECTIVE

As announced on 1st April’2020, the Department of Biotechnology (DBT) desires to establish Country's First National Indian Biological Data Centre (IBDC) for Bio Science related data deposition, storage, annotation and sharing of such data generated in the country through extensive funding from various Government Organizations. The IBDC will house the required infrastructure and technical skills for storage of biological data and distribution through an appropriate web portal. The IBDC will enable life science researchers, to deposit biological data in a central repository and thus safeguard data generated using public resources from loss. The IBDC will be hosted in the Regional Centre for Biotechnology, Faridabad and National Informatics Centre-Bhubaneshwar. The IBDC

will be created through a collaboration between Regional Centre for Biotechnology, National Institute of Immunology, International Centre for Genetic Engineering & Biotechnology-New Delhi with help from the National Informatics Centre and support from the Department of Biotechnology, Ministry of Science & Technology, Government of India. The work associated with the present tender document includes all activities associated with construction of a new data centre at the Regional Centre for Biotechnology, Faridabad and procurement/integration of IBDC hardware to be housed at the National Informatics Data Centre in Bhubaneshwar.

C. GENERAL REQUIREMENTS

I. All proposed hardware, software (released commercially or as open-source) and infrastructure must be supported by the Supplier at the time of system acceptance and throughout the subsequent 60 months of production system use.

II. The entire proposed system, including all, compute nodes, support nodes (login, data transfer, system management), networking, and storage must be a balanced, commercially-available, production-grade HPC system that contains an appropriate combination of processor, memory, interconnect, disk input/output (I/O), and operating system (OS) capabilities to execute complex, tightly-coupled, large-scale scientific calculations; more specifically, the system must be able to successfully execute a variety of workloads, including jobs which stress all subsystems and which require the simultaneous, tightly-coupled use of the full number of compute nodes within the system.

III. All hardware/equipment must be new; no refurbished or used hardware/equipment is allowed.

IV. All nodes and operating systems that are provided must include any required fixes for Spectre/Meltdown vulnerabilities till its life cycle.

V. The vendor must carry out the installation, commissioning and cabling of all the hardware as well as software components as a project in totality.

VI. The vendor must pay visit to NIC Bhubaneshwar Data Center and RCB Faridabad to assess the available site and infrastructure to commission hardware/equipment. A new data centre has to be built in the designated space provided at the Regional Centre for Biotechnology.

VII. Once the award is complete, the supplier must provide a resource similar to a project manager who shall be nodal point for execution of entire project for the entire duration of the project as per detailed scope of work mentioned into this tender document.

VIII. The bidder must provide an escalation matrix for problem resolution and standard resolution timeline for integration and commissioning related issues.

IX. The bidder must provide list of resources to be deployed for successful execution of the project.

X. The bidder must ensure that execution team is certified for all type of IT equipment's configuration and installation as per technical specifications asked for.

D. SCOPE WILL COVER THE FOLLOWING

- Site Survey
- Preparation of Design layout
- Preparation of Approach document

- Building of Civil and electrical infra at RCB
- Supply, Installation, Integration, testing, and commissioning of IT hardware as per technical specifications.
- Supply, Integration & Deployment of eco system (power and cooling)
- Inspection, Testing, Audit & Certification (Tier-II & above)
- Adhering to the norms & specifications mentioned in the tender document
- Trial Run & Acceptance
- Warranty, end to end support and services
- Maintaining the IBDC for 03 years including 02 years' additional warranty support
- Training to the staff on various aspects in monitoring and maintaining the IBDC

a) LAYOUT ARCHITECTURE / DRAWINGS

The details of the proposed layout architecture at the two sites should be provided with the technical bid. On the award of work order under this work, the contractor shall immediately proceed with the preparation of drawing according to the work order to be carried out. **Two sets of such working drawings including make of all items shall be submitted to RCB for its approval to ensure that work will be carried out in accordance with specification and proposed drawing including such changes as may have been mutually agreed upon. All the drawings shall be submitted to the Client for their approval within 10 days of award of work**. In addition, the contractor must furnish detailed bar chart showing the various activity w.r.t. time and must organize co-ordination meeting at the site to review the progress of work.

b) BROAD SCOPE AND DESIGN PARAMETERS

The layout is made such that, there is a scope to add one more row to meet the future requirements. Bidder should supply and deploy all the components mentioned under this bid document, ensure the smooth functionality of the same, provide warranty and operational services as stipulated in the bid.

The scope of the bid is divided based on the site requirement i.e. NIC Bhubaneshwar Data Center and RCB Faridabad.

NIC Bhubaneshwar scope will be as follows:

- Supply, installation, testing, and commissioning of miscellaneous component in IBDC as per Technical specifications.

RCB Faridabad scope will be as follows:

- Detailed scope and specifications of Civil works
- Deployment of Electrical equipment, cabling, conduits, fittings and fixtures
- Supply, installation, testing, and commissioning of miscellaneous component in IBDC as per Technical specifications.

c) TRIAL RUN AND ACCEPTANCE

Upon successful inspection and testing, the equipment shall be put on trial run for at least for a period of 48 hrs. for various components. Acceptance Criteria:

i. Hardware should be from original manufacturers and should be shipped in original packing with OEM part numbers.
ii. All supplied Hardware shall undergo Power on Self-Test (POST) for bidder should

arrange at least 48 hrs on full IT load and load.

iii. OEM should showcase the heat load test on the quoted Cooling solution.

iv. OEM should also showcase the redundancy functionality on the quoted cooling solution.

v. Bidder/OEM should provide training to all desire members of NIC Bhubaneshwar & RCB Faridabad on the quoted Solution.

vi. Bidder/OEM should get successful installation and commissioning certificate from NIC Bhubaneshwar & RCB Faridabad.

vii. Bidder should showcase the functionality of the quoted items/ components.

d) TECHNICAL REQUIREMENTS

The submitted bid must contain and cover the technical aspects provided below.

I. The HPC setup contains multiple distinct (i.e. mutually exclusive) sets of nodes/servers and other hardware as given below and specified in the hardware technical specification section.
   - Compute Nodes
   - Login Nodes
   - System Management nodes
   - GPU nodes
   - High-Speed Network Infrastructure
   - High-Capacity Storage System

II. The data center setup to be installed at RCB, Faridabad consists of site preparation, civil work and required electrical/UPS and cooling system as specified in the technical specification section.

III. The vendor must work with RCB/NIC to submit all relevant documentations like high level and low-level design documents, SOP documents, etc.

IV. Installation and commissioning including Hardware racking, stacking, cabling and Power on Self-Test (POST) of supplied compute nodes, switch hardware and other components and sub-systems at end-user site and demonstration of benchmark results as stipulated.

V. On all the nodes, the vendor will install the latest stable version of RHEL. The compute nodes should be able to rebuild through network install with a kick-start file from the master node.

VI. Bidder will also install IB, GigE, and Storage sub system.

VII. The operating system, HPC cluster management software, workload management software, monitoring tools, SLURM job scheduling software and other software will also need to be installed.

VIII. **Demonstration of HPL benchmark on the CPU & GPU nodes of the HPC infrastructure.**

IX. The System Integrator/OEM must ensure for seamless software integration compatibility between cluster and storage management applications.

X. Documentation and Manuals of all systems to be supplied.

23.TECHNICAL SPECIFICATIONS AT NIC BHUBANESWAR DATA CENTER

Note: at NIC Bhubaneswar, the existing Rack's dimension is 600mmX1000mm. The devices should be supplied with C13/C14 power cables to connect to the PDU of racks.

If the Storage solution is incompatible with the existing RACKs, then new RACKs (max. up to 2 no.) must be provided at NIC data centre.

Technical specifications for Server (Node-1)			
Make & Model :			
Sr. No	**Items**	**Descriptions**	**Compliance Yes / No**
1	Chassis	Max. 4U Rack Mountable Chassis with 8 x 2.5" Bay	
	CPU	Server should be configure with 4 x Intel Xeon-Gold 6240L (2.8GHz/16-core/150W) Processor or higher	
	Motherboard	Intel C621 Chipset or higher	
	Memory	Server should be configured with 32 x 128GB DDR4-2933 RAM Server scalability should be at least 6TB, 48 DIMM Slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	HDD Bays	Server to be populated with 4 x 960GB SATA SSD (min. 3 DWPD). The drive carrier should have an automatic alert mechanism to avoid data-loss/downtime.	
	Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB battery backed write cache (onboard or on a PCI Express slot)	
	Networking Connectivity	1 x Dual 10Gbe Base-T network adaptors with additional Port for Management 4 x 1Gb Network port 2 x singleport InfiniBand HDR 100 Gbps	
	Interfaces	Micro SD slot - 1/M.2 Drives with RAID1 4 Nos. of USB Ports with at least 2 USB 3.0	
	Power Supply	Server should have redundant 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply or equivalent power supply	
	Fans	Redundant hot-plug system fans	
	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support, USB 2.0 Support Energy Star	

		ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum)	
	System Security	UEFI Secure Boot and Secure Start supportSecurity feature to ensure servers do not execute compromised firmware codeFIPS 140-2 validationCommon Criteria certificationConfigurable for PCI DSS complianceAdvanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browserSupport for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithmsTamper-free updates - components digitally signed and verifiedSecure Recovery - recover critical firmware to known good state on detection of compromised firmwareAbility to rollback firmwareSecure erase of NAND/User dataTPM (Trusted Platform Module) 1.2 optionTPM (Trusted Platform Module) 2.0 option	
	Operating Systems and Virtualization Software Support	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), VMware, CentOS	
	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2. Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
	Embedded Remote Management and firmware security	1.System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. Should support RESTful API integration 6. Server should support agentless management using the out-of-band remote management port 7. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 8. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay -	

		Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.	
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware	
	Chassis CPU	The Systems Management software should provide Role-based access control	
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like Memory and HDD.	
		Availability of the firmware rollback feature in quoted server i.e. in case a wrong /malicious firmware up-grad happens on a server, have option to roll back to the last upgrade which was working fine.	
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	

Technical specifications for Server (Node-2)			
Make & Model			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
2	Chassis	Max. 4U Rack Mountable Chassis with 8 x 2.5" Bay	
	CPU	Server should be configure with 4 x Intel Xeon-Gold 6242 (2.8GHz/16-core/150W) Processor or higher	
	Motherboard	Intel C621 Chipset or higher	
	Memory	Server should be configured with 8 x 128GB DDR4-2933 RAM or 32 x 32GB DDR4-2933 RAM. Server scalability should be up to 4TB & 48 DIMM slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	HDD Bays	Server to be populated with 4 x 960GB SSD (min. 3 DWPD). The drive carrier should have an automatic alert mechanism to avoid data-loss/downtime.	
	Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB	

		battery backed write cache (onboard or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption	
	Networking Connectivity	1 x Dual 10Gbe Base-T network adaptors with additional Port for Management 4 x 1Gb Network port 2 x singleport InfiniBand HDR 100 Gbps	
	Interfaces	Micro SD slot – 1 USB 3.0 - 4	
	Power Supply	Server should have redundant 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply or equivalent power supply	
	Fans	Redundant hot-plug system fans	
	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support USB 2.0 Support Energy Star ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum)	
	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option	
	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware CentOS	
	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover	

		and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
	Embedded Remote Management and firmware security	1.System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware. 4. Server should support agentless management using the out-of-band remote management port 5. Should support RESTful API integration 6. Server should support agentless management using the out-of-band remote management port 7. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 8. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.	
	Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data centre. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware	
		The Systems Management software should provide Role-based access control	
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like Memory and HDD.	
		Availability of the firmware rollback feature in quoted server i.e. in case a wrong /malicious firmware up-grad happens on a server, have option to roll back to the last upgrade which was working fine.	

		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	

Technical specifications for multi-GPU server (Node -3) – <u>Please refer "Annexure – A" of the Corrigendum</u> for revised Configuration			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
3	Processor	2x Intel Xeon Gold 6248 20 core, 2.5GHz CPU or better	
	System Memory	Min. 768 GB (12 x 64 GB) 2933MHZ DDR4 or better. The Server should have minimum 24 DIMMs slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	GPU	8 x GPUs (Tesla V100) 32 NVLink	
	Performance	On or above 1 Peta-FLOPS mix precision	
	GPU Memory	256 GB (8X32) total system	
	CUDA Cores	Approx. 5000 **per GPU**	
	Tensor Cores	Approx. 600 **per GPU**	
	Power Requirements	4-6kW or less with hot-plug & redundant power supply	
	Rack space	4-6U or less	
	Storage	OS: 2X 960GB SATA SSDs (min. 3 DWPD) with additional 15 TB Storage on 10k SAS HDD. 16 hot pluggable drive bays within the same server form factor.	
	System Network	1 x Dual 10Gbe Base-T network adaptors with additional Port for Management	
		2 x singleport InfiniBand HDR 100 Gbps	
		4 x 1Gb Network port	
	GPU communications protocol	NVLink 2.0/ configured in hybrid cube-mesh NVLink network topology. NVSwitch providing 2.4 TB/s bi-section bandwidth.	
	Controller	It should support Integrated or add-on PCIe 3.0 based 12G SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB of Flash backed write cache onboard.	
	Interconnect	System should support 10G Ethernet, 100G EDR / HDR and 100G OPA Adapters. System should support min. 4nos of 100G EDR/HDR/OPA adapters.	
	Power supply fan	Server chassis should have dual redundant N+N (N > 1) hot pluggable single phase 220v-240v minimum 2200W power supply and redundant fan	
	OS Support	Red Hat Enterprise Linux /CentOS/ Ubuntu Linux	
	USB Port	2	
	RS232 Serial Port (in built or with accessory)	1	
	VGA Port	1	
	Ethernet (RJ45) Ports Operating	2	

	Temperature Range Software Support (Directly from OEM with updates & upgrades).	Normal AC temperature	
	Software Support (Directly from OEM with updates & upgrades). Support portal should be enabled for min. 3 users. Partner has to help build first model on-site with limited data-set	CUDA toolkit CUDA tuned Neural Network (cuDNN) Primitives TensorRT Inference Engine DeepStream SDK Video Analytics CUDA tuned BLAS CUDA tuned Sparse Matrix Operations (cuSPARSE) Multi-GPU Communications (NCCL), Kubernetes TensorFlow , Caffe , PyTorch, Theano, Keras, caffe2, CNTK	
	Time to Train a ResNet-50 model on 1.28Million images	Not more than 150 minutes. Published on respective OEMs website with quoted server model.	
	Time to Train a SSD model on 118K images.	Not more than 30 minutes. Published on respective OEMs website with quoted server model.	
	Time to train a GNMT model on 4.5M sentence pairs of English-German.	Not more than 20 minutes. Published on respective OEMs website with quoted server model.	
	Scalability & Cluster software Other features and operation support	System should be scalable with multi node cluster. Software support & cluster tools to be supplied along with product.	
	Scalability & Cluster software Other features and operation support	i. The solution given for ML/DL workload should be certified by the respective OEM vendor to act as verified, tightly coupled architecture. Public document for the same should be available or to be given as a Self-Certification by the Server OEM	
		ii. The solution should have ready to use container for different Big-data, ML, DL stack optimized for given architecture and configured to utilize GPUs fully.	
		iii. The solution provided should be highly scalable and should have reference architecture available for testing.	
		iii. The solution provided should be highly scalable and should have reference architecture available for testing.	
		iv. Proposed architecture should be tested and verified by the OEM and an undertaking for the same to be submitted on OEM letterhead. The undertaking should also state that the architecture (combination of Server/storage/network) is designed to get best-optimized performance, deployment to be made quickly and have minimum overheads.	

		v. The proposed solution should be cloud scalable in future.	
5	Management	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. 2. Server should have dedicated 1Gbps remote management port 3. Server should support agentless management using the out-of-band remote management port 4. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support. 5. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 6. Cloud bursting support, GUI management, Node provisioning and Installation wizard	
		The solution should have ready to use container for different Big-data, ML, DL stack optimized for given architecture and configured to utilize GPUs fully.	
		i. The solution given for ML/DL workload should be certified by the respective OEM vendor to act as verified, tightly coupled architecture. Public document for the same should be available. All the supporting document for the same should be submitted along with bid.	
		ii. The solution should have ready to use container for different Big-data, ML, DL stack optimized for given architecture and configured to utilize GPUs fully.	
		iii. The solution provided should be highly scalable and should have reference architecture available for testing.	
		iv. Proposed architecture should be tested and verified by the OEM and an undertaking for the same to be submitted on OEM letterhead. The undertaking should also state that the architecture (combination of Server/storage/network) is designed to get best-optimized performance, deployment to be made quickly and have minimum overheads.	
		v. The proposed solution should be cloud scalable in future.	
		vi. Proposed OEM should have min. 3 installation with similar system for Deep learning & Machine learning in different institutes (preferably in Education institutes, IITs, IISc, NIC, CSIR/DRDO/ISRO labs, large private players working in ML/DL etc.) with min. of 8 GPUs per node.	

		SI should have office in NCR & should have Engg. certified on Deep learning (Profile of Engg. to be attached). SI must support in initial project once annotated data is available with institute in choosing the right model and train the model using popular open source frameworks for a period of 1 year on-site. The topics for training should include the usage of GPU libraries/applications such as CUDA toolkit, CUDA tuned Neural Network (cuDNN), Primitives TensorRT Inference Engine, DeepStream SDK Video Analytics CUDA tuned BLAS, CUDA tuned Sparse Matrix Operations (cuSPARSE) Multi-GPU Communications (NCCL), Kubernetes TensorFlow , Caffe , PyTorch, Theano, Keras, caffe2, CNTK etc.	
		SI must provide 5 days training on system administration, Deep learning & Machine learning, Frameworks, Practical's with few popular modules & Inferencing.	

Technical specifications for Server (Node -4)			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
4	Chassis	2U or Higher Rack Mountable Chassis with 8 x 2.5" Bay	
	CPU	Server should be configure with 4 x Intel Xeon-Gold 6242 (2.8GHz/16-core/150W) Processor or higher	
	Motherboard	Intel C621 Chipset or higher	
	Memory	Server should be configured with 4 x 128GB DDR4-2933 RAM or 16 x 32GB DDR4-2933 RAM. Server scalability should be up to 4TB & 48 DIMM slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	HDD Bays	Server to be populated with 4 x 960GB SSD (min. 3 DWPD) The drive carrier should have an automatic alert mechanism to avoid data-loss/downtime.	
	Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB battery backed write cache (onboard or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption	
	Networking Connectivity	1 x Dual 10Gbe Base-T network adaptors with additional Port for Management 4 x 1Gb Network port 2 x singleport InfiniBand HDR 100Gbps	
	Interfaces	Micro SD slot – 1 USB 3.0 - 4	
	Power Supply	Server should have redundant 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply or equivalent power supply	
	Fans	Redundant hot-plug system fans	

	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support USB 2.0 Support Energy Star ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum)	
	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option	
	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware CentOS	
	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
	Embedded Remote Management and firmware security	1.System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and	

		software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware. 4. Server should support agentless management using the out-of-band remote management port 5. Should support RESTful API integration 6. Server should support agentless management using the out-of-band remote management port 7. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 8. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.	
	Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data centre. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware	
		The Systems Management software should provide Role-based access control	
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like Memory and HDD.	
		Availability of the firmware rollback feature in quoted server i.e. in case a wrong /malicious firmware up-grad happens on a server, have option to roll back to the last upgrade which was working fine.	
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	

Technical specifications for Server (Node-5)			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**

5	Chassis	2U or Higher Rack Mountable Chassis with 8 x 2.5" Bay	
	CPU	Server should be configure with 4 x Intel Xeon-Gold 6242 (2.8GHz/16-core/150W) Processor or higher	
	Motherboard	Intel C621 Chipset or higher	
	Memory	Server should be configured with 4 x 128GB DDR4-2933 RAM or 16 x 32GB DDR4-2933 RAM. Server scalability should be up to 4TB & 48 DIMM slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	HDD Bays	Server to be populated with 4 x 960GB SSD (min. 3 DWPD) The drive carrier should have an automatic alert mechanism to avoid data-loss/downtime.	
	Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB battery backed write cache (onboard or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption	
	Networking Connectivity	1 x Dual 10Gbe Base-T network adaptors with additional Port for Management 4 x 1Gb Network port 2 x singleport InfiniBand HDR 100GBps	
	Interfaces	Micro SD slot - 1/M.2 Drives with RAID1 4 Nos. of USB Ports with at least 2 USB 3.0	
	Power Supply	Server should have redundant 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply or equivalent power supply	
	Fans	Redundant hot-plug system fans	
	Industry Standard Compliance	ACPI 6.1 CompliantPCIe 3.0 CompliantPXE SupportWOL SupportMicrosoft® Logo certificationsUSB 3.0 & 2.0 SupportEnergy StarASHRAE A3/A4UEFI (Unified Extensible Firmware Interface Forum)	
	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option	
	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware CentOS	

	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
	Embedded Remote Management and firmware security	1.System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware. 4. Server should support agentless management using the out-of-band remote management port 5. Should support RESTful API integration 6. Server should support agentless management using the out-of-band remote management port 7. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 8. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.	
	Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data centre. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware	
		The Systems Management software should provide Role-based access control	
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	

		Should help provide proactive notification of actual or impending component failure alerts on critical components like Memory and HDD.	
		Availability of the firmware rollback feature in quoted server i.e. in case a wrong /malicious firmware up-grad happens on a server, have option to roll back to the last upgrade which was working fine.	
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	

Technical specifications for Server (Node-6)			
Make & Model :			
Sr. No	**Items**	**Descriptions**	**Compliance Yes / No**
6	Chassis	2U or Higher Rack Mountable Chassis with 8 x 2.5" Bay	
	CPU	Server should be configure with 4 x Intel Xeon-Gold 6242 (2.8GHz/16-core/150W) Processor or higher	
	Motherboard	Intel C621 Chipset or higher	
	Memory	Server should be configured with 4 x 128GB DDR4-2933 RAM or 16 x 32GB DDR4-2933 RAM. Server scalability should be up to 4TB & 48 DIMM slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	HDD Bays	Server to be populated with 4 x 960GB SSD (min. 3 DWPD) The drive carrier should have an automatic alert mechanism to avoid data-loss/downtime.	
	Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB battery backed write cache (onboard or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption	
	Networking features	1 x Dual 10Gbe Base-T network adaptors with Management Port. 2 x singleport InfiniBand HDR 100 Gbps 2 x 1Gb Network port	
	Interfaces	Micro SD slot - 1/M.2 Drives with RAID1 4 Nos. of USB Ports with at least 2 USB 3.0	
	Power Supply	Server should have redundant 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply or equivalent power supply	
	Fans	Redundant hot-plug system fans	
	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support	

		USB 2.0 Support Energy Star ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum)	
	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option Runtime Firmware Validation - Periodically scan essential firmware for compromised code during runtime	
	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware CentOS	
	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware	
		The Systems Management software should provide Role-based access control	
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like Memory and HDD.	
		Availability of the firmware rollback feature in quoted server i.e. in case a wrong /malicious firmware up-grad happens on a server, have option to roll back to the last upgrade which was working fine.	

		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	
	Embedded Remote Management and firmware security	1.System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware. 4. Server should support agentless management using the out-of-band remote management port 5. Should support RESTful API integration 6. Server should support agentless management using the out-of-band remote management port 7. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 8. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.	

Technical specifications for Tape Library

Make & Model :

Sr.No	Items	Descriptions	Compliance Yes / No
7	Drive Technology	LTO	
	Drive Generation	LTO 8	
	Tape Library expandability	Tape Library expandability- Minimum 80 Cartridge slots and shall be scalable to 280 slots or more within the same library and add up to 6 Expansion Library Modules.	
	Tape Drives Slot populated	Tape Library shall be configured with 6 x FC LTO-8 drive scalable to minimum of 20 drives	
	Base Model Form Factor	21U or higher rack form factor	
	Type of Connectivity	Tape Library shall provide native Fiber connectivity to SAN Environment	
	Connectivity Interface	8Gb Fiber Channel ports	

	Compression Ratio	2.5:1	
	Transfer Rate (TB/hour)	Native Transfer rates of up to 300 MB/s per LTO-8 Tape Drive native. Library shall preferably conform to the Data rate matching technique for higher reliability	
	Accessories	1. Appropriate quantity Required for LC to LC Multi-mode OM3 2-Fiber 5.0m Fiber Optic Cable. 2. 80 LTO-8 cartridges and Barcode Label Pack & reader	
	Cleaning Cartridge	At least 5 no. of Universal Cleaning cartridges	
	Data Cartridge	Tape library shall be offered with - Minimum 80 Cartridge slots and shall be scalable to 280 slots or more within the same library. Out of 80 slots, Tape library shall have at-least 5 Mail slots and shall be scalable to more than 30 mail slots, when fully populated.	
	Power Supply	Redundant Power Supply	
	Misc.	Tape Library shall provide web based remote monitoring capability	
		The proposed data cartridges should be configured with case/cover	
		All Cartridge slots shall be serviced by a common robotic arm	
		Tape Drive Architecture in the Library should preferably conform to INCITS/T10 SCSI-3 standard or newer standards	
		Optional - Library shall offer optional WORM support and embedded AES 256 bit encryption	
		Library shall be provided with a hardware device like USB key , separate appliance , Application Managed Encryption (AME) etc. i.e. The offered solution must be industry standards methods like USB / LME or AME to keep all the encrypted keys in a redundant fashion	
		Tape Library shall have partition support so that each configured drive can have own partition and allocated slots. Tape Library shall have support for at-least 20 partitions	
		SAN Switch should be part of solution to connect the tape library	
		Tape Library shall have GUI Front panel	
		Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action	
		Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved	

Technical specifications for Storage (4.5PB)			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
8	**Eligibility Criteria**	1) Entire storage solution must be from single OEM having L0, L1 & L2 support capability in India with 24x7 support services. Single OEM must be able to support both file system and storage hardware by themselves up to fixing software bugs in file system and underlying RAID array, providing timely resolution. 2) Storage solution proposed must be certified to work with diverse computing architectures including X86-64 (Intel & AMD), NVDIA GPU BASED SYSTEMS computing servers with GPGPUs. or	

		proof of successful installations in the form of signed installation report with these CPU architectures. 3) Storage OEM must have deployed similar solutions in India. These sites must be under active support contract. Please submit proof of installation and customer contact details. 4) Disk Type storage should consist of NL-SAS/SAS 4 TB or higher capacity disks only.	
	Capacity Requirement	Bidder to supply 4.5 PB raw capacity parallel file system storage solution in single global namespace such that: 1.At least 450 TB of raw capacity must be supplied on SSD drives, to deliver minimum sustained write performance of 100 GB/s 2. Minimum 4PB of raw capacity configured using NL-SAS/SAS drives, to deliver minimum sustained write performance of 50 GB/s 3. Should be configured with RAID 6 (8+2) or equivalent with dual parity 4. Metadata capacity should be configured to accommodate at least two billion files 5. File creation capacity of minimum 80,000 files per second	
	Parallel File System	Only OEM commercially supported IBM GPFS or OEM supported Lustre to be quoted	
	Storage Architecture	Storage solution must have: 1) Minimum two active-active controllers with redundant power supply and fans to prevent cache data loss (if applicable) during power failures 2) Connectivity to computing cluster over RDMA capable 100Gbps HDR100 InfiniBand network 3) I/O servers and controllers must have redundant and highly available paths to computing cluster as well as backend disk enclosures. 4) Storage solution must support hybrid media with ability to incorporate SSD / NL SAS 5) Storage system must support global hot spares for NL-SAS / SSD disks.	
	Standard File system Features	Storage solution must support: 1) User & Group Quota 2) POSIX compliance 3) Fine grained locking so that multiple clients can read & write from the same file simultaneously. 4) Ability to read and write in parallel to same file and different files. 5) Data striping across multiple I/O nodes and RAID LUNS. 6) Ability to transparently recover from client, server and network failures without losing data. 7) Ability to configure all capacity in single namespace as well as ability to create small namespaces. 8) Offered storage solution must be able to aggregate up to 8x 100 Gbps InfiniBand network connections to the IB Switch without needing to mount separate file system per network port. Proof of network aggregation with relevant benchmarks must be submitted. 9) Entire file system namespace must be mounted inside application containers without needing root/super user privileges. 10) If any of the above storage features are licensed for capacity then, all licenses for entire capacity required to meet stated performance must be supplied.	

	Connectivity	Storage solution must offer minimum 8 ports or higher of RDMA capable 100Gbps InfiniBand ports (capable of operating with HDR InfiniBand specifications). Additionally, there must be minimum 1 port of 1Gbps Ethernet per storage controller for management and monitoring. Metadata information network path must be separate from the data movement network paths.	
	Rebuild Performance	Fast rebuilds: Storage must offer fast rebuild capability for replacing failed drives. Bidders must demonstrate rebuilding 10TB or higher capacity drive in less than 10 hours.	
	Multi-tenancy & security	1) Storage solution must support multi-tenancy and security available in the propose File system should be deployed 2) Storage solution must support security features to prevent untrusted clients for changing data via root squash. 3) Storage solution must provide audit logging facility to track actions on files & directories in the file system. At minimum, file system must support enabling audit logging on files/directory create, delete and renames.Any additional licenses required for all of above features must be supplied with appropriate bill of material in the tender response.	
	Single Pane of Glass monitoring	A single pane of glass monitoring solution must be offered with: - Ability to monitor file system and underlying storage arrays in same GUI dashboard. - Ability to show device health, performance, any alerts on a single dashboard - Ability to drill down on performance from clients, storage servers to controllers to disks - Ability to monitor storage usage for specific user or job in real-time.	
	High Availability & Redundancy	1) Entire storage solution must not have any single point of failure with high availability and redundancy offered at each layer of the I/O stack. 2) Entire Solution must be in balanced with respect to no. of I/O servers, network ports, backend connectivity etc. 3) Storage solution must have a minimum of two active controllers, hot swappable redundant power supplies and fans. 4) 1% of disk drives of PFS should be configured as hot online spare drives or capacity. 5) The proposed storage system should tolerate simultaneous failure of any two disks is a single RAID group. 6) 20TB or higher capacity in RAID1 or equivalent to be quoted as metadata on SSD.	
	Scalability	Entire storage solution must support scale-out configurations up to 50 PB in single global namespace using similar building blocks.	

	Benchmarking tools	Bidder must submit benchmarking report along with tender response with: 1) Open-source IOR benchmarks (https://github.com/hpc/ior/releases) running on 8 compute nodes with 1 MB transfer size, and file size double than total storage cache and I/O node memory with -vv (double verbose) parameters and POSIX file per process workload are to be used for all throughput testing. 2) MDTEST Version 1.9.3 (https://sourceforge.net/projects/mdtest/files/mdtest%20latest/mdtest-1.9.3/) to be used for all metadata performance benchmarks running on 8 compute nodes with minimum parameters of "-n 100000 -i 3 -vv -w 4096 -u". 3) Bidder should submit the IOR benchmark for 50GB/s write performance and 50GB/s read performance with 1 MB block size and file size must be double than storage & I/O servers memory. Benchmarks must be run on minimum 8 and 16 compute nodes. Storage solution must deliver parallel file system metadata performance of minimum 60,000 files creates/sec. Bidders must also submit output of IOR and MDTEST. 4) Bidder (OEM) should run the benchmark on 20 node PFS clients over 100G EDR 5) Detailed benchmark report should be submitted along with the bid.	
	Infrastructure requirement for storage	1) Tender response must include detailed information on peak power consumption, cooling required, heat generated, number of racks used, rack dimension, rack clearance, number of PDUs per rack with ampere & voltage rating, no of electrical sockets and type of sockets required to connect PDUs, weight per rack, number of InfiniBand & Ethernet ports required per rack and any other relevant information to complete the deployment.	
	Warranty Support	Entire storage solution with Next Business Day parts delivery. All software & firmware upgrades and updates for storage array, parallel file system and monitoring & management components must be freely available to customer without any additional cost during warranty period.	
	Management & Monitoring	If the proposed storage system is composed of a number of external servers for various services, the storage management system software must be able to monitor and manage these servers, with at least centralized boot/shutdown capability. If additional software is required to manage these external servers, tenderers shall provide that software with enough licenses for the storage system. Please describe the functions and mechanisms of the required software.	
	Misc.	Necessary cable and connectors as per solution requirement should be provided.	
		Bidder must provide peak power in KW, heat in BTU/Hr, weight in Kg and airflow in CFM for cooling of the storage solution.	
		The OEM will be responsible for Supply, installation, configuration, commissioning, testing, maintenance and support for both hardware and software during the warranty period.	
		The installation/ integration should be done by OEM engineers only.	

Technical specifications for Backup Software			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
9	Backup Specifications	Proposed Solution should be a user-friendly enterprise console that enables the administrator to manage the complete backup and recovery environment via a Web-based interface with Active Directory, Azure AD or LDAP Integrated Authentication. This should allow the administrator to navigate, logon and perform functions at ease even from remote location	
		The proposed backup solution shall support industry leading cluster solution such as MSCS, MC Service Guard, and Veritas Cluster The Backup master system must support the following systems: Linux (x8664) 5.x/6.x/7.x & Windows 2012/2012R2/2016/2019 and Client System must support include: Windows, Linux, AIX, Solaris, HP-UNIX and Mac OS X Platform	
		The proposed backup software should use web-based scheduler for the backup jobs and efficient navigation without traveling across several pages, so most operations can be performed from a single screen. The proposed backup software should support both backups using snapshot/hardware based and software based as well as backup to tapes for long term and offline data retention	
		The proposed backup solution shall be configured in such a fashion that no extra license for client and media servers is required while moving from LAN to SAN based backup.	
		The proposed backup solution shall be configured with unlimited client and media licenses for both SAN based backup and LAN based backup.	
		The backup software should support the Capacity based model or Application based model of licensing.	
		The proposed backup solution supports the capability to write up to 32 data streams.	
		The proposed backup solution support de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restores operation to servers.	
		The proposed backup solution has in-built media management and supports cross platform device and media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media.	
		Backup software should have their own de-duplication technology in software based platform, which should be tightly integrated with backup solution to provide in-line or source-side or target side variable block level deduplication to achieve highest storage reduction methods for backup data retention. Backup & De-Duplication Software should be Hardware agnostic	
		Backup solution along with De-Dupe technology shall support simple backup replication strategy to keep the data off-site against any site failure with dis-similar target Hardware, which also should have bandwidth optimization without network WAN Optimizer	

		The Backup solution shall include Minimum of 500 TB of Usable space scalable to more than 2PB raw space using 4/8TB drive, where CPU or Hardware Change should not impact Licensing for running backup on physical servers, Virtual machines (Hyper-V, VMWARE, Citrix, Oracle Virtual Machine, etc.) and above database support with inclusive License for BMR on Windows, De-Duplication, Compression, Encryption (CAST-128, AES-256 or CAST-256), Backup Replication and Multi-Site Management. Where provided Disk Based De-Dupe Platform Should support Advanced Global De-dupe Engine, Replication and Encryption enabled Platform to maintain Backup Retention and Backup Archival Policy	
		The backup software should be capable to supporting 99,999 backup sessions in day. The proposed backup software should support both backups using snapshot/hardware based and software based as well as backup to tapes for long term and offline data retention. The backup software should be capable of supporting 1000 concurrent sessions. The backup software should be able to support maximum of 40 Million files per directory. The proposed backup software should support the data protection laws of the region (encryption, data security and user rights management). The proposed backup solution supports the capability to write up to 32 data streams. The proposed backup solution should support tape mirroring of the same job running concurrently with primary backup.	
		The proposed backup solution has certified "hot-online" backup solution for different type of Enterprise databases and applications.	
		~~The Proposed solution should be able to Identify, Classify and Protect Structured Data from Central location/Database allowing the appropriate level of privacy controls using data masking and supports Format Preserving Encryption (FPE) at the application/DB level which should be applied in place or archive according to its sensitivity and usage needs.~~	
		Online Dbase archiving should provide availability of database applications & Streamlines database backup, recovery, and cloning operations	
		Restores entire dbase archive runs or individual transactions back into production. Safety checks are performed to make sure the data is inserted correctly without jeopardizing production database integrity.	
		Should support database masking for security compliance	
		The proposed backup solution should allow state-of-the-art search capability enables fast and granular searches of its backup index for backup and restore. Include fast-search capabilities for metadata (name, mod date, type, etc.) and save-sets with offline indexes in your search results	
		Backup Solution must have Single sign-on (SSO) features to Log into Backup Software using your AD logon credentials along with Role-based access control to regulates operations administrators	
		Backup Solution must have Client package push install functions and Take advantage of AD/LDAP authentication to enable "push install" for backup agent on clients machines	

		Proposed solution may support complete BMR backup with incremental/differential snapshots for virtual machines running on Hyper-V 2008/2008R2/2012/2012R2/2016 and Vmware ESX Version 5.X/6.5	
		Should have specific agents to perform "hot" backups on the following databases, applications and Bare Metal Recovery such as:	
		Should meet the following Media Management capabilities	
		a. Allow Backup Disk Storage and Tape Library sharing among Client servers without additional license	
		b. Allow individual Tape Storage sharing among media servers and allow for reconfiguration without rebooting media servers	
		c. Tape drive support should be for SAS, iSCSI and Fiber based connections.	
		Ability to integrate with storage NAS snapshot based protection mechanisms & Integrated SAN Snapshot functions by providing WEBGUI Based control. Must support storage protocols such NDMP (version 3 & above) with Direct Access Restore, 5way NDMP Backup Support	
		Proposed solution should support push client feature for agent installation & agent less protection for Physical Machine Including support for VMware, Hyper-V, AHV, KVM & RHEL	
		The Proposed solution should be able to Identify, Classify and Protect Structured Data from Central location/Database allowing the appropriate level of privacy controls using data masking and supports Format Preserving Encryption (FPE) at the application/DB level which should be applied in place or archive according to its sensitivity and usage needs.	
		Online Dbase archiving should provide availability of database applications & Streamlines database backup, recovery, and cloning operations	
		Restores entire dbase archive runs or individual transactions back into production. Safety checks are performed to make sure the data is inserted correctly without jeopardizing production database integrity.	
		Should support database masking for security compliance	
		The proposed backup software should use the same API for software and hardware deduplication.	
		The backup software should support backup to disk /VTL / Deduplication Device via fibre channel or IP.	
		The proposed backup software should support both on premise and secure hosted backup solution.	
		The proposed backup solution shall support automatic skipping of backup during holidays.	
		The backup software should support the option of prioritizing backups.	
		The backup software should support missed job execution.	
		The Backup software should be able to recover only critical volumes and later restore other volumes that were backed up in separate sessions.	
		Backup Software should be offered with AES 256 bit encryption licences	

		Implementation& Installation of entire solution to be done only by OEM Professional Services Team	
		24x7 Premium Support to be provided	
		The backup server (including software & hardware) as per the best practice of the backup software OEM should be provided by the bidder	
		Reporting Features:	
	Monitoring & Reporting	a) Backup Software shall offer Extensive reporting capabilities to monitor the health of Backups. Shall support HTML, TEXT, XLS, PDF and CSV outputs. It shall support scheduled automated generation of the report on a daily basis.	
		b) The backup software must provide near real time monitoring and reporting of the backup environment. It should provide a graphical representation and monitoring of trends and current status.	
		c) Software shall support event notification to notify backup administrator about events like Job Failed or Job aborted etc.	

Technical specifications for Network Switches			
Infiniband (IB) Mellanox Quantum HDR Edge Switch			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
10	Switch Specifications	Switch architecture should be fixed form factor fitting 19" ETSI rack.	
		Switch should be pure Data Center class switches supporting latest DC technologies.	
		40-port Non-blocking Managed HDR InfiniBand Smart Switch in a 1U switch	
		Switch should support full bi-directional bandwidth per port.	
		Backward compatible to previous speeds	
		Switch should have internal redundant power supplies and fans from day one.	
		Should support 80 gold+ and energy star certified power supplies	
		Switch should support non-blocking wire speed performance on all ports	
		1+1 redundant & hot-swappable power	
		16Tb/s aggregate switch throughput	
		The switch should support latency less than 90ns port to port.	
		The system shall operate without degradation of performance between 0°c and 40°c	
		Should support features such as static routing, adaptive routing, congestion control and VL2VL mapping with enhanced VL mapping to enable modern topologies (SlimFly, Dragonfly+, Torus).	
		Should support 4x48K entry linear forwarding database	
		Should support 9 virtual lanes(8 data + 1 management)	

		Should be Compliant with IBTA 1.21 and 1.3.	
		Should support 256 to 4Kbyte MTU	
	Modules & Accessories	Switches should be provided with all the relevant mounting & connecting accessories. All necessary connecting cables and other accessories need to be provided along with switch.	
		Necessary connecting DAC cables, splitter cables and transceivers supporting and other associated accessories to be considered as part of solution & must be provided along with switches.	

10G Ethernet LAN Switch			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
11		Shall be 1 RU, 19" Rack Mountable	
		Switch should have minimum 48 x RJ-45 Copper,10GBASE-Ts with6 x 40GbE uplinks	
		Switch should support 6 x QSFP each port supporting 40GbE or 410GbE with breakout cable.	
		Switch should support hot-swappable redundant power supply with 4+1 redundant fan modules.	
		Switch shall have Switching Capacity of 720 Gbps and forwarding rate of 1 Bpps.	
		Switch should support latency less than 720ns or platform supports 1000 ns again depends on packet size	
		Should support min 8 GB NAND flash, 8 GB RAM as system memory.	
		Should support buffer memory of 16MB per switch	
		Shall have minimum 16K MAC Addresses.	
		Shall have minimum 1000 Active VLANs and 4,000 VLAN Ids support	
		Should support STP, RSTP, PVST, and PVRST modes.	
		Should support MLAg/vPC.	
		Should support VRR or VRRP.	
		Should support IGMP and MLD snooping	
		Shall have 802.1p class of service, IP differentiated service code point (DSCP).	
		Supports static and dynamic routing protocols (OSPF/OSPFv3/BGP)	
		Switch should support hybrid cloud connectivity with QinQ and VXLAN tunnels.	
		Supports Port Admin Edge and BPDU guard feature.	
		Should support 802.1x authentication and accounting with Dynamic VLAN assignment.	
		Switch should support IPv4 and IPv6 ACLs.	
		Configuration and management through the CLI, GUI, console, Telnet and SSH	
		Supports SNMPv2/3	
		Network Time Protocol(NTP) or equivalent support	
		Supports LDAP authentication, TACACS+, and RADIUS AAA.	
		Switch should support software upgrades via TFTP or FTP	
		IEEE 802.1 ab Link Layer Discovery Protocol (LLDP) support	
		Link Aggregation Control Protocol (LACP)	

		Switch should be IPv6 Certified/IPv6 logo ready/IPv6 ready	
		should be ROHS-6 compliant	
	Accessories & Support	Switches should be provided with all the relevant mounting & connecting accessories. All necessary connecting cables and other accessories need to be provided	
		Necessary connecting cables and transceivers supporting 10/40G and other associated accessories to be considered as part of solution & must be provided along with switches.	

Management Switch			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
12	Management Switch	Shall be 1 RU, 19" Rack Mountable	
		Switch should have minimum 24 nos. 10/100/1000 Base-T ports with additional 2 nos.1/10 gig SFP uplink ports	
		Switch should support 2 redundant, hot-swappable AC PSUs.	
		Should support 1 x RJ-45 serial console, 1 x RJ-45 100/1000BASE-T management port.	
		Switch shall have minimum 80 Gbps of switching fabric and 95 Mpps of forwarding rate.	
		Shall have minimum 16K MAC Addresses.	
		Shall have minimum 1000 Active VLANs and 4,000 VLAN Ids support	
		Should support STP, RSTP, PVST, and PVRST modes.	
		Should support MLAg/vPC.	
		Should support VRR or VRRP.	
		Should support IGMP and MLD snooping	
		Shall have 802.1p class of service, IP differentiated service code point (DSCP).	
		Supports static and dynamic routing protocols (OSPF/OSPFv3/BGP)	
		Switch should support hybrid cloud connectivity with QinQ and VXLAN tunnels.	
		Supports Port Admin Edge and BPDU guard feature.	
		Should support 802.1x authentication and accounting with Dynamic VLAN assignment.	
		Switch should support IPv4 and IPv6 ACLs.	
		Configuration and management through the CLI, GUI, console, Telnet and SSH	
		Supports SNMPv2/3	
		Network Time Protocol(NTP) or equivalent support	
		Supports LDAP authentication, TACACS+, and RADIUS AAA.	
		Switch should support software upgrades via TFTP or FTP	
		IEEE 802.1 ab Link Layer Discovery Protocol (LLDP) support	
		Link Aggregation Control Protocol (LACP)	
		Switch should be IPv6 Certified/IPv6 logo ready/IPv6 ready & should be ROHS-6 compliant.	

		Switches should be provided with all the relevant mounting & connecting accessories. All necessary connecting cables and other accessories need to be provided	
		Necessary connecting cables and transceivers supporting 10/40G and other associated accessories to be considered as part of solution & must be provided along with switches.	

Technical specifications of IP Based KVM with display unit for already existing RACKS			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
13	Easy Operation	Three port selection methods: Manual (via front panel pushbuttons), Hotkey, and multi-language OSD (On Screen Display). Multi-language keyboard support includes US English, UK English, etc.	
	Auto Scanning and Broadcast Mode	Auto Scan provides hands-free monitoring of selected devices at changeable speeds. Broadcast Mode sends commands from the console to all computers – allowing you to perform operations (such as software installations, upgrades, shutdowns, etc.), on all computers simultaneously	
	Superior Video Quality	Supports video resolutions up to 1920 x 1200 @ 60 Hz up to 30 meters, 1600 x 1200 @ 60 Hz up to 40 meters, and 1280 x 1024 @ 75 Hz up to 50 meters*	
	Multiple User Accounts	Supports up to 10 user and 1-administrator accounts. Two-Level password security – supports one administrator and ten user profiles. Password protection prevents unauthorized access to the installation Multiplatform support – Windows, Linux, Mac and Sun	
	Form Factor	One KVM console controls up to 8, 16, or 32 directly connected computers This space-saving innovation means that can be conveniently installed in a 1U system rack.	

Technical Specification for Firewall (Qty. - 2 nos.)			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
		Security Features	
	General & Security Features	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	
		Firewall appliance should have at least 8 x 1GE RJ45 interface and 2 x 10G SFP+ interfaces	
		Firewall throughput should be at least 35 Gbps and it should have minimum 5Gbps VPN throughput	
		Firewall should support 2000 site-to-site & client to site VPN Tunnels	

14		Firewall should support minimum 500 concurrent SSL VPN users and should be scalable in future. The OEM should provide VPN Client software for 500 users and should support various operating systems like Windows, Linux/Ubuntu and Mac	
		Firewall should support 5 Million concurrent sessions and 2,00,000 new sessions per second	
		The solution should support minimum 3.5 Gbps of NGFW (FW + IPS + AVC) throughput for Mix / production traffic	
		The solution should support minimum 3 Gbps of Threat Prevention (FW + IPS + AVC + AV) throughput for Mix / production traffic	
		Proposed Solution must support IPv6 and should have IPv4 to IPv6 transition. The proposed solution should be able to cater the clients/systems connected with IPv4 after the migration of NGFW to IPv6	
		The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode	
		The proposed system should have integrated Traffic Shaping functionality	
		The proposed system should support: IPSEC VPN, PPTP VPN and L2TP VPN	
		The device shall utilize inbuilt hardware VPN acceleration: (a) IPSEC (DES, 3DES, AES) encryption/decryption and (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 should support site-to-site VPN configurations with Route/Policy based IPSec tunnel	
		The system shall support IPSEC site-to-site VPN and remote user VPN	
		The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN	
		Intrusion Prevention System	
		NSS recommendation for complete device or IPS cabability	
		IPS throughput should be minimum 4 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 a configurable actions 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	
		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 solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole 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	
		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	
		High Availability	
		The proposed system shall have the capability for high availability (HA) features as 2 no. firewall has proposed for NIC Data Centre	
		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	
		Should have dedicated hardware/virtual appliance/client software for logging and reporting solution along with required-licenses	
		Real-time display of information for analyzing real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic	
		The firewalls management system shall support the option of exporting logs in CSV/XLS, XML and syslog and also capable of export into PDF	
		The firewall management system shall support real-time log forwarding in syslog and CSV formats	
		The firewall management system should support sending of customized usage & performance reports through mail at	

		defined schedules such as daily, weekly, monthly or predefined time	
		The firewall shall offer inbuilt management feature through https, SSH, CLI etc. or centralized management with integrated log server. The proposed system shall have the capability for high availability (HA) features as 2 no. firewall has proposed for NIC Data Centre.	
		The firewalls management system shall support detection and notification of performance degradation such as critically high CPU and memory utilization and when maximum supported number of concurrent sessions reached	
		The firewall should have hot swappable redundant power supply units	
15	REDHAT	REDHAT Linux Standard	

24. TECHNICAL SPECIFICATIONS AT REGIONAL CENTER FOR BIOTECHNOLOGY, FARIDABAD

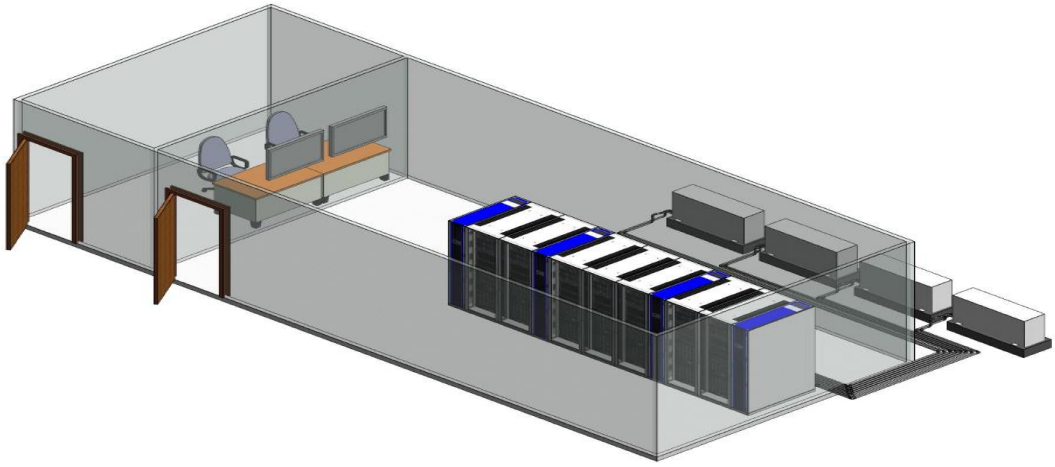
A. INFRASTRUCRE REQUIREMENT

The detail specifications of the IBDC Solution, 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 essentially includes internal redundant or backup power supplies, environmental controls (e.g., precision air conditioning, fire suppression, smoke detection, water leak detection, humidity sensor, intelligent monitoring system, security devices, etc.) Air-conditioning system is to have 100 % reliability on 24 x 7 basis with a total cooling capacity (15 Ton) and with adequate standby for system redundancy. (Failure of any single unit; still to meet the total cooling requirement of estimated load). The ambient temperature considered for the calculation of total tonnage requirement should be 45 Degrees Adequate RAW power supply and earthing in the server room will be provided by the customer.

B. DETAILED SCOPE AND SPECIFICATIONS OF CIVIL WORKS

i. Walls and Partitions
ii. DC Entrance and Emergency exit doors
iii. Inline/ In row Cooling assembly
iv. Cooling system
v. Fire resistance False floor/ False ceiling
vi. Cold Aisle
vii. Racks with IPDUs
viii. Biometric Access Control
ix. Environment Monitoring Systems
x. IBDC Surveillance System
xi. Smoke detection & Fire suppression
xii. Rodent and Repellent
xiii. Lighting Arrestor



Tentative Diagram for RCB data centre

C. WALLS AND PARTITIONS

The identified are for IBDC is mix of brick wall and glass panels. Bidder should cover the entire glass panel area (rear side) with Fire retardant Gypsum blocks.

The newly constructed wall should be just before the glass panel. The wall need to be painted with Fire rated and permissible white colour to get a look of a single wall. The wall should be made from bottom of the DC ground to slab level. No wooden/card board partitions are allowed.

To meet the current requirement, IBDC room will be housed with 7 racks in a single row. It is required to construct Cold Aisle with appropriate doors on both sides of the rows. To meet the current requirement, IBDC room will be housed with 7 racks in a single row. It is required to construct both Cold & hot Aisle with appropriate doors on both sides of the rows. The construction of Cold & hot Aisle with appropriate in-row cooling units with redundancy (Failure of any single unit; still to meet the total cooling requirement of estimated load). Cut-outs in the walls / partitions / false floor and false roof at required places shall be provided for Electrical and Data cabling entry to the IBDC room and such entry / exit points need to be sealed.

D. SPECIFICATIONS OF FIRE RATED BRICKS

Make: Gypsum Blocks,
Standards: Fire rated bricks adhering to European and British EN 12859 Standard.
Fire Standards: The wall should offer 2 hrs. F-30-A & BS-476 Fire Protection.

E. COLD AISLE CONTAINMENT SYSTEM

- Data Center should be equipped with high performance DX Gas Based in rack cooling system with Hot and Cold aisle system within the rack.
- Fire Retardant / Rated Toughened Glass need to be used for the front doors so that the Cold Aisle area is clearly visible from both sides of the Aisle. The rear doors should be of split type CRCA door Fire Detection & suppression units are to be housed to cover the Cold and Hot Aisle.
- The Entire containment should be sealed & properly insulated to avoid mixing of Cold Air and Hot Air directly.
- All Hardware required would be standard as per manufacturer's standard specifications.
- The material used for construction of Cold Aisle should comply with UL standards.
- Doors should open to the outside of Cold aisle

F. TECHNICAL SPECIFICATIONS OF INFRASTRUCTURE

AIR CONDITIONING

- IBDC server and network racks should be equipped with cooling units to provide closed loop precision cooling system which should be able to cool the equipment is uniformly right from 1st U to 42nd U of Rack through In-Row Based Cooling system.
- The Data centre required total 60 KW (40 KW for the calculated required load with additional 50% (i.e. 20 KW) higher capacity) cooling capacity of each unit minimum 20 KW with N+1 redundancy. Data Center should be equipped with high performance DX Gas Based in rack cooling system with Hot and Cold aisle system within the rack. It should have heat exchanger to remove high levels of waste heat from server enclosures

and provide uniform, effective, affordable cooling for Servers and similar IT equipment (switches etc.) installed in server enclosures. Each DX Gas cooling system should be a closed unit consisting of a cooling system. The design of the unit should be optimised for use in data centres. The integrated DX Gas Based heat exchanger minimum 300 mm wide should have cooling output of up to Minimum 20 kW, combined with standard server enclosure dimensions, the lowest possible weight and comprehensive possibilities for monitoring.

- The air/Gas Based heat exchanger should be mounted on the side of the rack. Cooling system Rack DX Gas Based should have enclosure-based cooling separate from the room air and should also reduce the noise level. The hot server air should be drawn off to the rear of the server rack. After cooling should deliver air horizontally and should cover entire 42 U height of the Rack as servers would draw air based on the heat load of the servers.
- he system should have integrated with minimum 3 Nos. EC fans (cooling output 20KW or higher) to achieve maximum efficiency and minimise the electrical energy consumption. A full fan configuration should be utilised to achieve redundancy or to minimise power consumption. The system should be based on standard integrated software/controller concept that provides automatic control of the specified server air intake temperature. Infinitely variable cooling Gas Based flow rate & fan speed should be there for precise matching to the power losses of the components installed in the IT rack.
- The optimum operating point should be achieved with minimum energy consumption. It should have intelligent sensor network to monitor the air and Gas Based temperatures, as well as the Gas Based flow rate and leakage management. It should incorporate temperature sensors for the hot and cold air with integrated fail-safe mode. The monitoring and alarm management for all physical parameters should be realised via SNMP and Ethernet.

- **AIR COOLED CONDENSERS**

It may be read as "Redundant true online UPS System, the redundancy and demand adequate capacity to serve the entire IT equipment's (Server, Storage, network etc.) installed inside Data Centre'.

Parameters	Required Performance	Complied (Yes/ No)
Air throughput of fans	4800 m3/h or better	
Cooling output	Minimum 20 kW	
Duty cycle %	100%	
Cooling medium	R410a	
Dimension	300W x2000Hx1200D or as per OEM Design	
Fan	EC	
No. of fan per unit	4 Nos. or as per OEM Design	
Compressor	Speed Regulated / Variable capacity	
Quantity	4 Nos.	
Protection category	IEC 60529 IP 20	

- Note: Bidder should submit a certificate from OEM of data centre cooling equipment / heat exchangers that all cooling components quoted conform to their standards and specifications.

EVAPORATOR
REFRIGERANT CIRCUIT

The circuit includes: Liquid line shut-off valve, charge connection, liquid line sight glass, filter dryer, Electronic expansion valve, safety valve, pressure transducers to relay information on high and low pressure values and relative condensing and evaporating temperatures for display on the controller, high and low pressure switches.

AIR FILTRATION

- The filter filters shall be minimum 30% efficient per ASHRAE Standard 52.1, UL Class 2 (MERV 8 per ASHRAE 52.2) or specific or OEM standard. Filters shall be EN779 G4 efficient. The pleated filters shall be replaceable from the rear of the unit.
- Clogged filter alarm must be available for standard.

HUMIDIFIER

The unit fitted with Humidifier shall be able to modulate/control the capacity and Humidifier shall be On/Off type. The humidifier shall be self-contained, steam-generating type, factory piped and wired, with disposable cylinder and automatic solid-state control circuit. Humidifier canisters shall be replaceable. The humidifier controller shall communicate directly to the microprocessor controller and provide complete status and control at the operator interface. Humidifier shall control flush cycling and conductivity via automated controls. Humidifier shall be capable of to meet the min/max. Technical requirement of steam per hour.

ELECTRONIC EXPANSION VALVE

The use of this accessory is particularly indicated for units that operate in very unstable heat load conditions or in unstable functional mode, as in the case of joint management of air conditioning and production of high temperature water. Use of the electronic thermostatic valve in fact allows to:

a) Maximize the heat exchange to the evaporator
b) Minimize response times on load variation and on operative conditions
c) Optimize the regulation of the over-heating
d) Guarantee maximum energy efficiency

CONTROLS AND SAFETY DEVICES

a) Manually resettable high-pressure gauge;
b) High pressure safety valve;
c) Antifreeze probe on each evaporator outlet;
d) Required controls and safety devices for DX Gas based systems should be provided.
e) Compressor and fan over temperature protection.

OPTIONAL (FOR CORROSIVE ENVIRONMENTS)

Copper / aluminium condensing coil treatment with passivized aluminium and polyurethane-based coating. The treatment consists of two layers, the first an aluminium passivation agent acting as a primer, and the second a polyurethane-based surface coating. The product is highly corrosion-resistant and can support almost any environmental conditions, including marine installations, rural environments, industrial areas and urban environments.

TESTING

All units are factory tested and supplied complete with oil and refrigerant charge or shall be filled at site. Computer Software generated technical data sheet should be attached with the offer. If required, the same needs to be demonstrated during the time of final approval.

NOISE LEVEL

The Cooling units should be designed for Low Noise Operation. The noise level of the Cooling units should not be more than 57 dBA (sound pressure values measured at 10 meters distance from the unit in free field and at nominal working conditions, in compliance with ISO 3744).

MONKEY MESH

The outdoor Cooling units including water/cooling pipes and other equipment which will be kept outside of the building should be fenced in order to protect it from monkey or other animal. The fencing wire used in mesh should be corrosion resistant and as per industry standards

WORK GUIDELINES

a) Civil work/MS framework for indoor and outdoor units related to AC, all cuttings should be properly finished as existing surrounding. The installation of outdoor unit in the building should be checked up structurally & their mounting should be structurally safe. Due care shall be taken by the bidder towards the following works:
   - Cutting of walls and floors/ ceiling, making holes, Sleeves. Foundation.

b) Piping & Pump
   - All piping and fitting should be triple layer PPR and all instrumentation Brass/MS
   - The pump shall be fully protected, regulated, and activated by the microprocessor control system and the electrical panel.

G. DEPLOYMENT OF ELECTRICAL EQUIPMENT, CABLING, CONDUITS, FITTINGS AND FIXTURES

SCOPE:

- Deployment of HT Panel and its cabling work. The desired/ applicable HT Panel must be including in the scope of work if needed.
- UPS and Batteries, Ageing factor for batteries required one (unity)
- Static Transfer Switching unit (STS)
- Power Distribution Panels
- Overhead Bus Bar System with Tap-off for Rack Power
- Electrical cabling, fixtures
- General conditions (cabling/panels/Trays/ Conduits/Termination)

- Bidder should conduct the sites survey; identify the suitable place and space for placing various equipment's, running the power and data cables to DC.
- Bidder need to provide the Trays / GI / HDPE pipes to route the cables in a neat and cleaned manner.
- Bidder should supply the requisite base/ stands to mount the equipment for easy of cabling and protection from water leakages etc.
- UPS shall have built-in feature to test UPS at 100% Load without the need of any external Load Bank. In-case this feature is not available within the UPS, Vendor shall provide an External Load Bank equal to UPS Capacity which will be kept at the site till the Warranty period ends.
- The Uninterruptible Power Supply (UPS) systems are required to provide continuous, regulated AC power to the equipment of the Organisation, irrespective of any disturbances or disruptions occurring on the main power supply. Minimum 20KVA /20kw modular UPS modules in Single Frame. UPS system designed with N+N redundancy.
- This specification describes the modular UPS, a modular 60 kVA/60 kW Modular Three-Phase Uninterruptible Power Supply System - (minimum 20 KW modules) system for critical equipment applications. It defines the electrical and mechanical characteristics and requirements for a continuous-duty three-phase, solid-state, uninterruptible power supply system. The uninterruptible power supply system, hereafter referred to as the UPS, shall provide high-quality power.
- DB panel should be mounted on to utility rack/room wall with 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.
- Any extra electrical points and data points (additional provisioning of 10-15%) required in the server room shall have to be provided by the vendor at his own cost.
- UPS module shall be of modular design and construction consisting multiple number of hot pluggable type sub modules within the cabinet.
- Each sub module shall allow easy frontal draw-out accessibility for easy maintenance and low mean time to repair (MITR).
- In case there is no resumption of input power for a certain configurable time period & the UPS is running on battery, the UPS system must provide a remote alarm mechanism.
- UPS should operate in double conversion mode. Efficiency of the product at full load in Double conversion mode should not be less than 95% and in E-Conversion/ECO mode should not be less than 99%.
- UPS system should support 99.9999% uptime
- UPS should have redundant control module in case of one of the control module is down or UPS should have enough redundant modules to cater to the control module failures.
- UPS should be of online UPS with Pure sign wave.
- No power module should get non-functional in case of failure of controller.

TECHNICAL SPECIFICATION OF UPS

S. No	Parameter	Specification	Compliance (Yes/No)
1	Capacity (in KVA / KW)	60 kVA/60 kW Modular Three-Phase Uninterruptible Power Supply System-(at least 3 modules of appropriate capacity)	
2	Technology and Capability	a) True Online configuration double conversion UPS.	
		b) Modular UPS required with N no. of modules to complete the total requirement having N+1 redundancy over the module. Each Module must have its own controller.	
		c) DSP (Digital Signal Processor) / Microprocessor based control, using IGBT devices and high switching frequency PWM	
		d) PFC controlled IGBT rectifier with Active power factor	
		e) Capability to operate in N+N Redundant Configuration.	
		f) Each module should have independent controller or Microprocessor, display and static switch and each module should be User swappable control modules	
		g) The malfunction of one of the UPS unit's power or control modules shall cause that particular UPS unit to be automatically isolated from the system and the remaining UPS units shall continue to support the load. Replacement or repair of a UPS unit shall be achieved without disturbance to the connected load, while the remaining modules continue operating in online mode (online safe swap ability)	
		h) Dedicated and single Battery string should be available for each UPS Rack so that in the event of a malfunction (in the affected battery string or UPS) there is autonomy available through another UPS & its battery	
3	Temperature (design ambient)	0 to 40°C	
4	IP Class	IP20	
5	Acoustic Noise measured at 1 Mt distance	<70db	
6	Input facility -Phases / Wires	3-Phase / 4-Wire & Ground (R, Y, B -Phases & Ground)	
7	Nominal Input Voltage	340V to 460V.	
8	Nominal Input Frequency	40 – 70 Hz	
9	Input Frequency Range	50Hz (± 5%)	
10	Input Power Factor	> 0.99 on Full load	
11	Input Current Harmonic Distortion (THDi)	<3 % on Full Load	

12	ENVIRONMENTAL CONDITIONS	The UPS system shall be designed to operate continuously at full load without degradation of its reliability, operating characteristics or service life in the following environmental conditions:	
		Battery ambient temperature range 20°C to 25°C	
		Humidity (relative) 5 to 95% non-condensing	
		Storage: UPS -5 deg C to +50 deg °C;	
		The UPS system shall be designed for operation in altitudes up to 1000 metres, without the need for derating or reduction of the above environmental operating temperatures.	
		The audible noise generated by the UPS system during normal operation shall not exceed 70 dBA per module measured at 1 metre from the front of the UPS @ 100% load	
13	Generator Compatibility	Compatibility to gen set supply used for this project	
14		a) Input to Rectifier	
	Input Protection	b) Input to Bypass	
		c) Manual Bypass (In-built)	
15	Over voltage/under voltage	Specify	
16	Input Frequency variation protection	Specify	
17	Phase sequence change	The UPS should have Phase Sequence Correction at Input side for phase sequence change; UPS should continue to operate on Double Conversion Mode of Operation in case of Negative Sequence/Phase Reversal at Input of the UPS system.	
18	Nominal Output Voltage	380/400/415Vac (Three Phase Four-wire)	
19	Output Voltage Regulation	+/- 1%	
20	Nominal Output Frequency	50 Hz or 60 Hz	
21	Output Frequency	+/- 0.1% Hz (Free Running / Self Clocked Mode)	
22	Output Wave Form	Pure sine wave	
23	Output voltage distortion	<= 1.5% (For 100% Linear / Resistive Load)	
		<= 3% (For 100% Non-Linear)	
24	Crest Factor	Crest Factor - 3 : 1 or higher on Full Load	
25	Unbalanced load on phases	100% unbalanced load should be allowed	
26	Output Protection	Specify	
28	Output short circuit Protection.	Specify	
29	Over-temperature protection.	Specify	
30	Rectifier / Charger	Built-in, solid-state charger with appropriate ratings	

31	Battery Charger Ripple	Ripple of +/- 1%	
32	Overall Efficiency		
		shall be > 95.5 % @ 100% load or higher	
		95.5% @ 75% load or higher	
		95% @ 50% load or higher	
		94.5% @ 25% load or higher	
33	Transfer Time (Mode of operation)	Nil from Mains mode to Battery Mode	
		Nil from Battery Mode to Mains mode	
34	Automatic & Bi-directional static by-pass (In-built)	Should be provided to take care of uninterrupted transfer of load from Inverter to bypass (under overload / fault conditions) & automatic retransfer from bypass to inverter (on removal of overload / fault conditions)	
35	Inverter Overload capacity (Mains Mode &	125% for 10 minutes	
	Battery Mode)	150% for 60 seconds	
36	Backup Required	Each UPS module should have one battery string to support 30 Minutes backup (IT Full load is 40 KW (+50% extra i.e. 20 KW) total 60 KW. Dedicated single battery string should consist for each UPS so that in the event of a battery or UPS malfunction ensures autonomy by other UPS and Battery in redundancy.	
37	Battery Type	Sealed Maintenance Free (SMF), valve regulated	
38	Batteries are to be recharged	A fully discharged battery system shall be capable of being recharged to 80% of the UPS output capacity as per OEM & industry standards. Ageing for batteries required one (unity)	
39	Nominal DC bus Voltage	or as per design standard of Manufacturer	
40	Ripple voltage at full load	ripple of +/- 1%	
41	Battery charging with temp. Compensation	Should be available	
42	Type of battery charging circuit.	Constant Voltage with Current Limit 1.65 to 1.8 auto adjustable with load % (back-up time). However, Battery sizing should base on end cell voltage from 1.75 V to 2 V	
43	Automatic Battery Test	The UPS shall initiate an automatic battery testing sequence periodically (once a month), at a programmed day and time of day, selectable by the end user. The user will be able to able and disable the automatic battery test	
44	Bypass	the UPS	
45 46	Alarms and Status Information	All faults conditions to be displayed in LCD with alarm	
		(sound)	

47	Metering	Input Voltage (Line to Neutral)	
		Bypass Voltage (Line to Line and line to Neutral)	
		Output Voltage (Line To Neutral)	
		Output Current per Phase (L1, L2, L3)	
		Output Frequency	
		Output load current (%) (L1, L2, L3)	
		Output Load (%) Average	
		Output Real power (KW) (L1, L2, L3)	
		Output Apparent power (KVA)	
		(L1, L2, L3)	
		Battery Current (Charge/discharge)	
		Battery Voltage	
48	Communication ports	The UPS shall be able to communicate through RS232 and USB.	
	Network Communications	HTTP/SNMP/Mod-bus or 10/100Mbit Ethernet card should be include for SNMP communication over a local area network.	
		* Remote shut down * The function shall allow the user to disable all UPS (Modules) outputs in an emergency situation * UPS monitoring software * UPS alarms & status changes detected on the spot 8 Real time monitoring & record of UPS measures * Email & SMS notifications * Local Network Monitoring System	
48	Width (in mm)	Specify	
49	Depth (in mm)	Specify	
50	Height (in mm)	Specify	
51	All Modes Protection	(L-L, L-N, L-G, N-G)	
52		UPS OEM must have inbuilt surge protection as per IEC standards	
53	Certifications	UPS OEM must have inbuilt surge protection as per IEC standards	
54	Credentials	UPS OEM must have inbuilt surge protection as per IEC standards	
56	standards	Should support the following standards	
		Safety Standard: IEC/EN 62040-1	
		Electromagnetic Compatibility Standard (EMC): IEC/EN 62040-2, Emission Class C2	
		Immunity Class C3	
		Performance Standard: EN 62040-3+B1:B2	
		The UPS shall be a true on-line double conversion, voltage and frequency independent (VFI) technology in accordance with standards EN 62 Wiring 040-3	
		Wiring practices, materials, and coding shall be in accordance with the requirements of the EN	

BATTERY BANK TECHNICAL SPECIFICATIONS:

S. No.	DESCRIPTION	PARAMETERS REQUIRED	Compliance (Yes / No)
1.1	Type	Valve regulated lead-acid (VRLA)-standard 2V cells, suitable for 30 Mins backup on full load i.e. Backup is required 30 mins on PF at 0.9	
1.2	Cell Containers	Polypropylene	
1.3	Cell Covers	Shall be permanently fixed such that the seepage of electrolyte gas escape and entry of electro static spark are prevented, it shall be fire retardant	
1.4	Plates	The OEM must be complies with MFX-for positive plate, Flat pasted positive & negative plates.	
1.5	Grid Growth Provision	This Provision should be made in the cell design to prevent failure due to internal shorting / rupture of cell because of grid growth.	
1.6	Separators	Shall be of Glass mat or synthetic material having high acid absorption capability, resistant to Sulphuric acid and good insulating properties.	
1.7	Pressure Regulating Valve	Each cell shall be provided with a pressure regulating valve.	
1.8	Terminal Posts	The surface of the terminal post extending above the cell cover including bolt hole shall be coated with an acid resistant and corrosion retardant material. Both positive and negative posts shall be clearly and unambiguously identifiable.	
1.9	Connectors, Nuts, Bolts, Heat Shrinkable sleeves	Non-corroding lead or copper connectors of suitable size shall be provided to enable connection of the cells. Nuts and bolts for connecting the cells shall be made of lead coated copper, brass or stainless steel. All inter cell connectors shall be protected with heat shrinkable silicon sleeves for reducing environmental impact including a corrosive environment.	
1.10	Flame Arrestors	Each cell shall be equipped with a Flame Arrestor to defuse the Hydrogen gas escaped during charge and discharge. Material of the flame arrestor shall not affect the performance of the cell.	
1.11	Battery Bank Stand & Cell Orientation	MS self-stackable racks with multi-tier & multi row arrangement. Ageing factor for batteries required one (unity)	
1.12	Capacity requirements	The battery voltage shall not be less than the following values, when a fully charged battery is put to discharge at C/10 rate.	
1.13	Type test of battery	1.After six minutes of discharge 1.98 V/ cell.	
		2.After six hours of discharge 1.92 V / cell.	
		3.After 8 hours of discharge 1.85 V/ cell.	
		4.After 10 hours of discharge 1.75 V/ cell.	
		Watt hour efficiency shall be better than 80%.	
		The bidder shall submit the type test certificates as specified as per relevant IEC standards or Type test report for 1530Ah as single cell highest rating.	

GENERAL SPECIFICATIONS OF UPS

Replacement or repair of a UPS module shall be achieved on line, without risk to personnel, and without disturbance or risk to the connected load.

UPS system shall be able to differentiate between overload and short circuit conditions and in case of any short circuit at output side, relevant ACB/MCCB shall trip and not the UPS.

To prolong battery life, the UPS shall have the facility for automatically adjusting the battery charging voltage according to the environmental temperature of the batteries. The battery charger shall be ripple-free avoiding premature battery ageing. Ageing for batteries required one (unity).

The UPS shall have built-in protection against under voltage, over current, and over voltage conditions, including low- energy surges introduced on the primary a/c source and the bypass source.

Fan redundancy: Redundant cooling fans need to be provided in UPS Protection: Built-in / External back-feed contractor for both, Mains and Bypass input or as per OEM standard.

H. ELECTRICAL WORK

Power Distribution for Server & Communication Room, Electrical Points, cabling etc.:

The Data Centre will be provisioned with UPS Power Distribution System along with MCBs. From the UPS distribution board, electrical cable will be drawn for distribution to the racks. The wiring will be carried out by the bidder by using fire retardant appropriate rating electrical cable, channels etc. For the cooling system, raw power is available at LT Panel (little far from the server room). The bidder is required to install distribution panel and need to connect from the LT Panel, which is used to connect the cooling system. The bidder may need to install additional DBs, if required.

Technical specifications

- Electrical main panel for data centre, NOC and UPS room.
- Dynamic voltage regulator (solid state) of capacity150 KVA as per required electrical power for cooling and UPS system other devices for Data Center
- UPS power distribution system as per data centre requirement.
- Cables for UPS to DB: Copper, 5core, 25sq.mm
- Cables for UPS DB to PDU & other points: Copper multi strands, 5 core, 4sq.mm
- Complete Single Line Diagram should be made and certified by the user before starting the work.
- The wiring will be carried out by the bidder by using fire retardant appropriate rating electrical cable.
- All power rating should be designed in consideration with all the devices involve inside server room.
- Complete distribution should not have any single point of failure.
- Complete distribution panel should be non-compartmentalized type, modular, totally shrouded.
- Bus bars should be of Electrolytic Grade Copper as per EN 13601
- Bus bar support and cover systems are fire retardant as per UL 94 V0.

Power Socket & Plug

Power Socket & Plug for Racks: Three Phase, indoor type IP 65 (latched), 32A, 3pin 2-pole + earth, three phase 415 volts, inter-locked Socket & Plug outlet similar to Lapp EPIC-Industrial connectors and must be technically complied.

Earthing:-

- Earthing required for electrical panel, UPS , UPS DB and Data Center in scope of bidders.
- Earthing should be zero volts,
- Separate Chemical based Earthing should be provided by Thick copper strip.
- Earthing solution should last for at least five years.

Network Cabling and Cable-Trays

- From each network, cabling required form server room to NOC & 50 no. workstations.
- Along with LAN cabling, the bidder should also design and lay cable- trays for Storage System up to the racks in the Data Centre.
- Bidder should ensure that all the cable raceways are adequately grounded and fully concealed with covers. The cables should be appropriately marked and labelled.
- The Data Centre should be equipped with separate ducts for power supply distribution and data/network cable. The duct should be designed in such a way that it is possible to do the retro fitment in future. The ducts should be positioned in accordance with the racks for structured and snarl free wiring. The size of the power cable duct and NOC cable duct should be such that it must be possible to accommodate Wiring needs for Servers. Each cable is required proper dressing and marking at both the ends.

Parameter	Specification/ Features Reqd.	Complied Yes/No
Cables & Conduit	The bidder shall install, terminate and connect up all cables & Conduits as per the drawing submitted/	
Cables	All cables shall be FRLS (Fire Retarded Low Smoke) type	
Insulation	The system of wiring shall consist of multi core PVC insulated standard copper conductor wires of suitable rating in metallic channels. All wiring shall be hidden and to be properly routed in existing false ceiling.	
Cable Laying	Cable shall generally be installed in ladder type; site fabricated/pre-fabricated trays except for some short run in rigid/flexible conduit for protection or crossing.	
Cable Tag & Marker	Each Cable shall be tag with number	
Tagging	Cable shall be tag at the entrance and exit from any equipment and junction box	
Cable Termination	The termination and connection of cables shall be done strictly in accordance with the drawing and in consultancy with RCB Faridabad.	
Channels	M.S. Channel, conduits, electrical panels and wiring, switches and sockets etc. shall conform to Indian standards for specifications and should be installed in consultation with RCB, Faridabad	
Type	Electrical system shall be intelligent type to enable their	

	integration and monitoring with BMS	
Earthing	Earthing of equipments, surge protector, including supply of earthing material, Lighting arrest and any other electrical safety measures, if required.	
Miscellaneous	All the electrical panels, Switches boxes, Sockets, wires etc. required for the Data Centre to be provided. All fittings should confirm to BIS	

INTERNAL COMPONENTS

The Panels shall be equipped complete with all types of required number of Air circuit breakers, switch fuse units, contactors, relays, fuses, meters, instruments, indicating lamps, push buttons, equipment, fittings, bus bars, cable boxes, cable glands etc. and all the necessary internal connections / wiring as required and necessary for proper complete functioning of the Panels shall be supplied and installed on the Panels. All part of the Panels carrying current including the components, connections, joints and instruments shall be capable of carrying their specified rated current continuously, without temperature rise exceeding the acceptable values of the relevant specifications at the part of the Panels. All units of the same rating and specifications shall be interchangeable.

I. FIRE DETECTION AND SUPPRESSION

Delivery of an active extinguishing system that detects and extinguishes fires in closed server and network cabinets. High-performance fan must extract air samples for smoke analysis into the system's measuring chamber. The integrated extinguishing system must trigger if the concentration of smoke exceeds the limits. The extinguishing process must not be electrically conducting and must be fast and residue-free. NOVEC 1230 must be employed as the extinguishing gas.

Fire detection and suppression system should be installed for server room and for racks with an appropriate amount of medium on the basis of room size. Three void system is required including false ceiling, false flooring and room. The system should contain the following: -

1. Fire alarm panel
2. Cylinder
3. Piping
4. Smoke detector
5. Fire nozzles
6. Medium NOVEC 1230
7. Acoustic alarm with light indication

Note:

- Protected area: The entire volume of the server racks shall be protected with fire detection and fire suppression system. The doors should be secured by Access Control system.
- Integration of both Access control system and Smoke detection system to un-lock all the doors in case of Fire and emergency is must.
- All sensor cables used should be of FRLS wires. Smoke detection and
- Fire detection Sensors.
- Each IT racks should be deployed with smoke detector and have capability to integrate and monitor with DCIM.

- 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 should be used to ensure that no harm to human beings and environment is caused.

J. BIOMETRIC ACCESS CONTROL

- Biometric Access control systems are to be placed to control the opening and closing of IBDC entrance and exit doors. Biometric Readers shall support both Finger Print and as well as card based authentication.
- Biometric Authentication Controller and Software should support Single, Dual Authentication with at least 10 combinations.
- Both these doors are Industrial design, Fire retardant doors. Accordingly, the controller (power) and Magnetic locks need to be taken care to handle the weight of the door.
- Supply should include Biometric access control systems with finger print scanners of two no. for each door as Authentication is required while entry and as well as exit.
- Biometric Controller and Software should be same for IBDC rack doors and as well as IBDC Entrance and Exit doors. Else, Bidder shall provide separate Biometric H/W, S/W for operating of rack doors.
- Software should have perpetual licenses. Software should work either on Windows or Linux platform.
- All the Authentication logs are to be stored for at least one year with a provision to back up the data.
- Biometric Authentication Controller should be integrated with Fire Controller to disable Authentication of all doors during Fire / Emergency.
- Biometric controller should have Ethernet (RJ45) port to communicate with supplied Software for storing of records, logs and events and should support remote logging / syslog.
- Supply should include sufficient and required readers, controller, Software and suitable electro-magnetic locks, required brackets, power adapters and cables.
- The supplied Access control units should provide interlocking facility
- Access control systems should be of tamper proof / mechanism to log the evidence of any tamper trials.
- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion and loss of access control etc.
- Inbuilt card reader
- Day, Date, Time and duration based access rights for user

Technical specifications of Biometric Reader with Keypad & Card

Templates	9,500
Integrated Proximity Reader	125KHz Multi-technology
PC to Reader /Panel to Reader	Ethernet (CAT5) / Wiegand (6 Cond. Shielded 18 AWG)
Dimensions /Weight	5.7” (145 mm) Wide X 4.92” (125 mm) High X 1.3” (33 mm) Deep / 12 oz. (340 g.)
Operating temperature /Humidity	32° F to +131° F (0° C to +55° C) / 0 - 95% RH

Power Requirements	DC 9~24V, 1A
Sensor (Resolution) /Template size	Optical (500 DPI) / 352 bytes
Authentication time Speed	≤ 4 sec
False Rejection /Acceptance Rate	0.01% / 0.001%
Features	LCD Display: 128 X 64 pixels; 2 LEDs; 10 number keys; 6 function keys; 1 bell button

K. CCTV SURVEILLANCE SYSTEM (NETWORK VIDEO RECORDER (NVR) SOLUTION)

- The bidder should propose a solution for IP enabled Closed Circuit Television System (CCTV) which will provide on-line display of video display/images on monitor. 6 Nos. Camera (Data Center and NOC) or higher should be used to view specific areas of interest and create a record for post event analysis.
- Video Operation Codec Management, Recording and Processing Software / Appliance NVR should be scalable, should offer a complete Video Surveillance solution that will be scalable to minimum 16 cameras that can be added as and when required.
- Camera must provide at least 100 degree or better angle view with minimum 2 Megapixel resolution or better with day night recording functionalities.
- Mode: Auto; Fluorescent; Indoor; Outdoor MPEG-4 I H.264 compression
- Minimum full frame (25fps/ 30fps) rate under high motion and all conditions.
- Should support Intelligent Motion Detection and Night Vision
- The camera should configurable remotely
- IP Cameras output should be compatible with the quoted Network Video
- Recorder (NVR) solution.
- IP Camera should support Power on Ethernet (POE)
- Cameras must be ceiling mountable and tamper resistant/evident/proof
- All upgrades and releases should be made available free of cost during warranty /AMC period.
- Surveillance storage for minimum 6 months recording after implementing RAID 5
- Rack mountable, maximum 4U size appliances along with rack mounting equipment / brackets etc.
- Supply should include the Software to view the output of selected cameras I-views etc.
- Note: Supply should include one no. 55" LED Panel for viewing of all cameras which are part of DC Surveillance system (Ref. section 15.2.1 for specifications).

LABELS: Engraved PVC labels shall be provided on all incoming and outgoing feeders.

NAME AND DANGER NOTICE PLATES: Notice plate shall be affixed on all Panels. The danger notice plate shall indicate danger notice.

L. MANUAL FIRE ALARM PULL STATIONS

- UL/ FM Approved
- Switch contact ratings: gold-plated; rating 0.25 A@ 30 VAC or VDC.

- Manual Fire Alarm Stations shall be non-code, with a key or hex- operated reset lock in order that they may be tested, and so designed that after actual Emergency Operation, they cannot be restored to normal except by use of a key or hex. An operated station shall automatically condition itself to be visually detected as activated. Manual stations shall be constructed of red coloured LEXAN (or polycarbonate equivalent) with clearly visible operating instructions provided on the cover. The word FIRE shall appear on the front of the stations in white letters, 1.00 inches (2.54 em) or larger. Stations shall be suitable for surface mounting on matching back box SB-10 or SB- I/0; or semi-flush mounting on a standard single-gang, double-gang, or 4" (10.16 em) square electrical box, and shall be installed within the limits defined by the Americans with Disabilities Act (ADA) or per national/local requirements. Manual Stations shall be under- writers Laboratories listed.
- **HOOTER / MINI-HORNS -** UL and ULC Listed CSFM, MEA and FM Approved

M. MONITORING SYSTEM:

A centralized physical infrastructure monitoring system which is capable to record historical data, events and send event details through email shall be provided to monitor & maintain the maximum up time for all the Infrastructure components inside the Data Center. Bidder should supply DCIM software that can integrate UPS. IPPDU, Cooling system. WLD, Fire system and other sensors for temperature and humidity. DC infrastructure/ power utilization efficiency of DC should be available real time.

- Centralized dashboard for complete DCIM
- Rack Based DX Cooling system management & control
- Temperature monitoring & controls at all specified positions
- UPS monitoring,
- IT rack's PDU monitoring.
- Safety & security integration.
- Fire system smoke detector.
- Temperature and humidity.
- Rack front door access.
- Rack rear door emergency opening.
- Data Center access control system.
- Water leakage detection system
- Protocol compliance : SNMP, Modbus or Canbus or Profibus, BACnet,
- Interface : Ethernet, RS-485, RS-232, Rs-484
- Capability to manage interdependencies between IT and other building equipment's to improve power utilization efficiency
- Other related accessories- SMS unit.
- No limitation on monitoring the number of devices

Specification of Monitoring Hardware

Monitoring should be an intelligent monitoring system with an Ethernet 10BaseT network connection. The priorities of the various functions are monitoring, controlling and documenting physical parameters inside the Server and network racks. These functions should be managed and

controlled via different protocols. Several input/output units (I/O unit) should be connected to one processing unit via a patch cable. This/these function module(s) should connect to the sensors via a standard plug connector. The sensors should be coded so that the function blocks recognize automatically which sensors are connected. Technical specifications:

Temperature Range	0^0C to 45^0 C
Operating humidity range	5% to 95% relative humidity, non-condensing
Sensor / CAN - Bus connection units	4 or more
Interfaces	Network Interface :(RJ 45): Ethernet to IEEE 802.3 via 10/100 Basset with PoE or other which fulfil the requirement without disturbing system architecture Mini USB for system setting. Serial interface: 1 x for connecting Display unit or GSM Unit or ISDN UNIT. User Interface: Integral WEB Server. Control room connection: Integral OPC Server.
Protocols	Ethernet :TCP/IPv4, TCP, SNMPv3, Telnet , SSH, , HTTP, HTTPS , DHCP , DNS Server, SNMPtrap, or NTP, or SMTP, or xml
Redundant power supply	Monitoring system should support redundant power supply
Main sensors	Main sensors latest temperature Sensor for Access control infrared technology sensors.

N. RODENT AND REPELLENT

Bidder should propose a rodent repellant solution which should drive away RODENTS using the principle of intense high frequency sound waves. The entire facility, including under access floor void and above false ceiling void should be- protected from rodents as they may gnaw away at the data, voice or even power cables causing a major downtime. The device installed should emit intensive ultrasound that is audible and painful to rodents, but is inaudible and harmless to humans. The device should make it undesirable for the rodents to inhabit or cohabit and leads to avoidance of the area being protected by ultrasound.

O. RACKS SPECIFICATIONS

Racks will be used to house all the IT Equipment's i.e. servers/network/storage/network devices. Rack is designed as per safety standards to withstand the modern IT infra requirement. Both front & rear door should be designed to give active high performance cooling system with handle lock system. Each Rack should include: Frame of sturdy frame section construction, consisting of min 12x folded rolled hollow frame section punched in 25mm DIN pitch pattern, PU Gasket Side panel, 1.5 mm with PU Gasket, Full Height 19", Angle, Top and Bottom Covers, two vertical IP PDUs.

Rack Specifications:

*** Rack should be compatible with hardware supplied**

Sl. No	Parameter	Specification	Qty.
1	Make	APC/ Rittal/ Vertiv or equivalent	7 No
2	Rack Height	42U	
3	Rack Width	19”	
4	Max Height	Max Height 2200mm including castors/wheels/plinth	
5	Max Width	600/800mm	
6	Max Depth	1200mm	
7	Color	Standard Color	
8	Front Door	Glass with unique lock	
9	Rear Door	Steel	
10	Load bearing capacity	1200 kg or higher	
11	Standard Warranty	Three (03) comprehensive onsite warranty support + two (02) years additional comprehensive onsite warranty support for repair or replace	

- All RACKS should be of same specifications
- Covered top and bottom
- Rear space saving spilt door with four point secure locking system
- Lockable & remove able side panels
- Front door with toughened glass with electromagnetic handle with digit electronic keypad system.
- Rear door sheet steel plain door with emergency auto door opening system.
- Stationary shelf-1 No/Rack
- Sliding Shelf – 1 No/Rack
- Surface finish: Nano ceramic coated, electro-dip coated primed to 20 microns and powder coated with texture polyester RAL 9005/7035 to 80 to 120 microns or similar
- Optimized for high capacity cable management system
- Cable access openings with pre-installed brushes.
- Complaint to all security & stability standards and provided integrated electrical grounding
- All seven nos. racks of data centre should be fitted with automatic rear door opening system; the door should open automatically in case of failure of the cooling system, high temperature and fire.
- Intelligent PDU (2 Nos. per rack):- Minimum specifications: - IP Based intelligent metered PDU socket strips: 3 phases 5 wire 440V, 50Hz, 32Amp PDU. Each PDU should have minimum 24 Nos. IEC C13 and 6 Nos. of C19 with appropriate display. Web server with HTTP, HTTPS (TLS 1.2), SMTP, SMTPS (TLS 1.2), ICMP, DHCP,

IPv4, IPv6, Syslog, SNMP v1/v2c/v3, JSON, JSON API, RSTP and integration with DCIM.

- Supply should include Server racks and 1 network racks.
- All the racks should have provision for cable trays to route the cables and Network racks should be housed with vertical cable trays in the front side of the rack.
- All the racks should have both front and back doors. Rack doors should have physical locks to provide physical security.
- KVM specification may be read separately.
- Should supports Windows, Linux, Mac OS9/OSX, Sun Microsystems
- On-Screen-Display (OSD) & Cascade Chain functions. The OSD with intuitive menus for quick and effective navigation.
- Advanced user profiles and configurable OSD hot key combinations & should support Multilingual OSD: at least English and /OR France/German/Spanish/ Italian/Russian/ Simplified Chinese/Japanese
- Racks should support efficient cooling mechanism with backend support of Cooling Units. Average rack power density is of around 10 KW per rack..
- Support resolution up to 1920 x 1080, SUN 1152 x 900 resolution compatible
  Auto Scan video for effortless monitoring, Supports LED display for PC and/or server status monitoring., Supports video resolutions Up to 1920 x 1080 / 1920 x 1200 when collecting to FHD 17" panel, Enable/disable beeper during channel switching.
- Expansion up to 128 servers by 8-level cascade (by 16-port KVM) from a single console. Cascaded units do not need special configuration.
  Hot-pluggable: all devices connected to KVM can be added or removed at any time without shutting down the devices.
- Easily switch between connected devices with: Hardware Push Button, Hot-Keys on USB keyboard, OSD menu. Hotkey combination: Scroll-lock, Cap-lock, Num-lock, Alt, Ctrl with Multi lingual on screen display menu
- Network racks need to be placed in the middle of each row with overlay tray connecting both the rows to run the network / data cables between the two rows.
- Each rack will be housed with two IPDUs.
- Blanking Panel: 50% each for all the supplied Racks.
- Supply should include the software to view all IPDUs and all the sockets in a single dash board view.
- Should support event logs, SNMP and syslog service for logging the event.
- Should support SMS / eMail to send alerts
- Certifications, Environmental and Safety Requirements-
  • Racks should be manufactured by ISO9001:2008, ISO14001:2004 & OHSAS18001:2007 Certified company and should have proper EHS Policy.
  • Product, grounding and bonding to be as per UL/EIA310D/DIN41494 standards
  • Manufacturer must certify that the products are RoHS Compliance.
  • Manufacturer must comply DIN41494 and Equivalent EIA 310/ISO/EN/CEA Standard.
  • The rack should comply minimum of IP 20 rating for protection against touch, ingress of foreign bodies and ingress of water.
  • The enclosure should both protect the user from mechanical hazards and generally

meet the requirements for a mechanical enclosure (stability, mechanical strength, aperture sizes, etc.) as defined in IEC 60950 Third Edition

GENERAL CONDITIONS (CABLING/ PANELS/PIPING/ TRAYS/CONDUITS/ TERMINATION)

- Except for inside, wherever the cable enters the DC or leaves the DC, the conduit end shall be sealed by suitable sealing compound having fire withstand capability.
- The cable end termination shall be carried out compression type cable glands, of adequate size.
- All the cables and conduit shall be tagged with numbers / labels / markers.
- Gaskets between all adjacent units and beneath all covers shall be provided to render the joints dust proof.
- Protection Class: All the indoor Panels shall have protection class of IP: 54
- Painting: The painting shall be seven-tank process with epoxy paint.

P. PLUMBING AND PIPING TO AUGMENT COOLING ARCHITECTURE

- Only DX Gas Based in rack cooling system has to considered, Chiller or related specifications to chiller are may not be considered.
- PPR pipes with required size need to be used. Piping should be done below the false floor.
- Outdoor Cooling Unit placement: Bidder should do the site survey to identify the place for housing the Outdoor Unit, Bidder should ensure requite platform / stand to mount outdoor cooling units. Power cabling need to be carried out by the bidder.
- Note: It is recommended to have Iron mesh covering the outdoor cooling units to avoid damage from external sources (animals).

CLEANING OF WORK SITE

The bidder shall, from time to time, remove all rubbish resulting from execution of his work. No materials shall be stored or placed on passage or drive ways. Upon completion of work, the bidder shall remove all materials to leave the premises clean and fit for use.

- All the cables laid outside should be armoured.
- Separate earthing cables need to be laid for providing earthing to the equipment and panels. Earthing should be zero volts, Separate Chemical based
- Earthing should be provided by Thick copper strip.
- Earthing solution should last for at least five years.

OTHER ROLES AND RESPONSIBILITIES OF THE BIDDER

- All the material used shall be one of the stipulated makes as per approved list of material.
- All dismantled material for which credit is not being given in the tender shall be handed over to the site engineer stored at proper place.
- Contractor shall be fully responsible for safety of his workers and in case of any accident / mishap; the entire responsibility shall be on the contractor.
- The work shall be executed without any loss / damage to the RCB's properties.
- The Bidder shall follow Change Management Procedures, Security Policies as

suggested by RCB.

- The Bidder shall co-ordinate with the selected ICT management team for ensuring continuity of operations. The Bidder should also support the selected ICT management team in diagnosing the problem from the Data Centre infrastructure end.
- The Bidder shall ensure proper handover / takeover of documents & other relevant materials in the event of change in personnel.
- All the internal review documents I reports used to monitor & execute the project should be shared with NIC Bhubaneswar Data Center and RCB, Faridabad as & when desired
- The Bidder shall proactively interact with other vendors / third parties / OEMs to ensure that the equipment is upgraded and maintained at a periodic interval. The Centre would only pay the energy bill (electricity charges) for operations and maintenance of the Data Centre.
- Miscellaneous work like civil mason work, cable tray, rails for electrical, and network cabling and other works required for proper functioning, aesthetics and durability of the DC infrastructure.
- Network cabling design layouts will be provided by the partner. The racks will be constructed of CRCA body structure for better strength and stability
- Bidder / DC Operations and Maintenance team shall abide by the IT Security Policies and Procedures of the Centers. No material shall be moved in-out, without prior permission of competent authority of NIC Bhubaneswar Data Center and RCB, Faridabad

Q. INFRASTRUCTRE DELIVERABLES (BOQ)

Technical parameter for all required items are mentioned in Data Center technical specification and these all should be complied technically. Required BOQ as below:

S. No.	Item Description	Unit	Qty
A	**Supply Part – Racks, IPPDU, Cooling, UPS, DCIM, Fire system and Security, Electrical and Civil work.**		
1	No. of Server and network Racks (42UH, 600/800mm Wide x 1000mm Deep or higher) and aisle containment 300mm each or higher	No.	7
2	PDU for racks with 20 Nos. IEC C13, 4 Nos. IEC C19 socket Zero U metered IP with 3 Mtr connection cable with industrial sockets	No.	14
3	Cooling unit (42UH, 300mm Wide x 1200mm Deep) with capacity (minimum 20 KW Each) in N+1 redundancy	No.	4
4	Low side work for four nos. cooing units.(piping, condensate hose, stand for outdoor unit, required insulation) per ckt length 50 mtr.	Lot	1
5	Modular and scalable UPS System – 60KVA/KW	No.	2
6	Battery with 15 Minutes backup	Lot	2
7	Fire suppression and detection system	No.	7
8	Acoustic for fire alarm system	No.	1
9	Light indication for alarm system	No.	1
10	Temp and humidity Monitoring sensors IP Based	No.	7

11	Rack front door with electromagnetic handle with digit electronic keypad system	No.	7
12	Rack Door access Sensor	No.	7
13	Emergency rear auto door opening system IP based	No.	7
14	Water Leak detection IP Based	Lot	1
15	DCIM software for single window console- Temp, Humidity, smoke, Rack front door access, emergency rear door, WLD, UPS system, Cooling system, IP PDU	Lot	1
16	Email Notifications	No.	1
17	SMS notifications	No.	1
18	Biometric Access Control for data center main door	No.	1
19	Blanking Panel for rack 1U size tool less	No.	70
20	IP NVR with 6 Nos. IP based camera with storage	Lot	1
21	Network cable for connectivity for server room to NOC.	Lot	1
B	**Electrical Work (At ground floor)**		
22	Dynamic voltage regulator (solid state) of capacity150 KVA	No.	1
23	Main row power distribution board	No.	1
24	UPS power distribution board qty. 2 or higher to avoid single point of failure	No.	2
25	Electrical cable and race ways, three phase power cable 02 Nos from Existing main control panel to data center	Lot	1
26	Earthing for Electrical panel, UPS panel, data center	Lot	1
	Civil work		
27	Data center and NOC partition	Lot	1
28	Data Center renovation- Painting	Lot	1
29	Two no. of console for NOC	No.	1
30	2 Nos. Chairs for NOC	No.	2
31	Data center and NOC room entry gate.	No.	1
32	55" monitor	No.	2
33	Fire rated false ceiling with light fixtures for DC and NOC	Lot.	1
34	Fire rated false flooring for data center	Lot	1
35	AC unit for UPS room, NOC and comfort cooling at server room	No.	5
36	Standard Comprehensive onsite warranty for three (03) year	Inclusive	1 no.
37	Additional Comprehensive onsite warranty for two (02) year	2 years	1 no.

R. TECHNICAL SPECIFICATIONS AT RCB (IT EQ)

Technical specifications for Server (Node-7)			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
16	Chassis	Max. 4U Rack Mountable Chassis with 8 x 2.5" Bay	
	CPU	Server should be configure with 4 x Intel Xeon-Gold 6240L (2.8GHz/16-core/150W) Processor or better	
	Motherboard	Intel C621 Chipset or higher	
	Memory	Server should be configured with 32 x 128GB DDR4-2933 RAM Server scalability should be at least 6TB.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	HDD Bays	Server to be populated with 4 x 960GB SSD. The drive carrier should have an automatic alert mechanism to avoid data-loss/downtime.	
	Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB battery backed write cache (onboard or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption	
	Networking Connectivity	1 x Dual 10Gbe Base-T network adaptors with additional Port for Management 4 x 1Gb Network port 2 x singleport InfiniBand HDR 100 GBps	
	Interfaces	Micro SD slot - 1/M.2 Drives with RAID1 4 Nos. of USB Ports with at least 2 USB 3.0	
	Power Supply	Server should have redundant 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply or equivalent power supply	
	Fans	Redundant hot-plug system fans	
	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support, USB 2.0 Support Energy Star ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum)	
	Operating Systems and Virtualization Software Support	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), VMware, CentOS	

	System Security	UEFI Secure Boot and Secure Start supportSecurity feature to ensure servers do not execute compromised firmware codeFIPS 140-2 validationCommon Criteria certificationConfigurable for PCI DSS complianceAdvanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browserSupport for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithmsTamper-free updates - components digitally signed and verifiedSecure Recovery - recover critical firmware to known good state on detection of compromised firmwareAbility to rollback firmwareSecure erase of NAND/User dataTPM (Trusted Platform Module) 1.2 optionTPM (Trusted Platform Module) 2.0 option	
	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2. Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
	Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Remote console sharing upto 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support RESTful API integration 8. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	

		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware	
	Chassis CPU	The Systems Management software should provide Role-based access control	
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like Memory and HDD.	
		Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
		Availability of the firmware rollback feature in quoted server i.e. in case a wrong /malicious firmware up-grad happens on a server, have option to roll back to the last upgrade which was working fine.	
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	

Technical specifications for GPU server (Node -8) <u>Please refer "Annexure – A" of the Corrigendum</u> for revised Configuration			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
17	Processor	2x Intel Xeon Gold 6248 20 core, 2.5GHz CPU or better	
	System Memory	Min. 768 GB (12 x 64 GB) 2933MHZ DDR4 or better. The Server should have minimum 24 DIMMs slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	GPU	8 x GPUs (Tesla V100) 32 NVLink	
	Performance	On or above 1 Peta-FLOPS mix precision	
	GPU Memory	256 GB (8X32) total system	
	CUDA Cores	Approx. 5000 **per GPU**	
	Tensor Cores	Approx. 600 **per GPU**	

	Power Requirements	4-6kW or less with hot-plug & redundant power supply	
	Rack space	4-6U or less	
	Storage	OS: 2X 960GB SATA SSDs (min. 3 DWPD) with additional 15 TB Storage on 10k SAS HDD. 16 hot pluggable drive bays within the same server form factor.	
	System Network	1 x Dual 10Gbe Base-T network adaptors with additional Port for Management	
		2 x singleport InfiniBand HDR 100 Gbps	
		4 x 1Gb Network port	
	GPU communications protocol	NVLink 2.0/ configured in hybrid cube-mesh NVLink network topology. NVSwitch providing 2.4 TB/s bi-section bandwidth.	
	Controller	It should support Integrated or add-on PCIe 3.0 based 12G SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB of Flash backed write cache onboard.	
	Interconnect	System should support 10G Ethernet, 100G EDR / HDR and 100G OPA Adapters. System should support min. 4nos of 100G EDR/HDR/OPA adapters.	
	Power supply fan	Server chassis should have dual redundant N+N (N > 1) hot pluggable single phase 220v-240v minimum 2200W power supply and redundant fan	
	OS Support	Red Hat Enterprise Linux /CentOS/ Ubuntu Linux	
	USB Port	2	
	RS232 Serial Port (in built or with accessory)	1	
	VGA Port	1	
	Ethernet (RJ45) Ports Operating	2	
	Temperature Range Software Support (Directly from OEM with updates & upgrades).	Normal AC temperature	
	Software Support (Directly from OEM with updates & upgrades). Support portal should be enabled for min. 3 users. Partner has to help build first model on-site with limited data-set	CUDA toolkit CUDA tuned Neural Network (cuDNN) Primitives TensorRT Inference Engine DeepStream SDK Video Analytics CUDA tuned BLAS CUDA tuned Sparse Matrix Operations (cuSPARSE) Multi-GPU Communications (NCCL), Kubernetes TensorFlow , Caffe , PyTorch, Theano, Keras, caffe2, CNTK	
	Time to Train a ResNet-50 model on 1.28Million images	Not more than 150 minutes. Published on respective OEMs website with quoted server model.	
	Time to Train a SSD model on 118K images.	Not more than 30 minutes. Published on respective OEMs website with quoted server model.	

	Time to train a GNMT model on 4.5M sentence pairs of English-German.	Not more than 20 minutes. Published on respective OEMs website with quoted server model.	
	Scalability & Cluster software Other features and operation support	System should be scalable with multi cluster. Software support & cluster tools to be supplied along with product.	
		i. The solution given for ML/DL workload should be certified by the respective OEM vendor to act as verified, tightly coupled architecture. Public document for the same should be available. All the supporting document for the same should be submitted along with bid.	
		ii. The solution should have ready to use container for different Big-data, ML, DL stack optimized for given architecture and configured to utilize GPUs fully.	
		iii. The solution provided should be highly scalable and should have reference architecture available for testing.	
		iv. Proposed architecture should be tested and verified by the OEM and an undertaking for the same to be submitted on OEM letterhead. The undertaking should also state that the architecture (combination of Server/storage/network) is designed to get best-optimized performance, deployment to be made quickly and have minimum overheads.	
		v. The proposed solution should be cloud scalable in future.	
	Management	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. 2. Server should have dedicated 1Gbps remote management port 3. Server should support agentless management using the out-of-band remote management port 4. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support. 5. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 6. Cloud bursting support, GUI management, Node provisioning and Installation wizard	
		The solution should have ready to use container for different Big-data, ML, DL stack optimized for given architecture and configured to utilize GPUs fully.	
		i. The solution given for ML/DL workload should be certified by the respective OEM vendor to act as verified, tightly coupled architecture. Public document for the same should be available. All the supporting document for the same should be submitted along with bid.	
		ii. The solution should have ready to use container for different Big-data, ML, DL stack optimized for given architecture and configured to utilize GPUs fully.	

		iii. The solution provided should be highly scalable and should have reference architecture available for testing.	
		iv. Proposed architecture should be tested and verified by the OEM and an undertaking for the same to be submitted on OEM letterhead. The undertaking should also state that the architecture (combination of Server/storage/network) is designed to get best-optimized performance, deployment to be made quickly and have minimum overheads.	
		v. The proposed solution should be cloud scalable in future.	
		vi. Proposed OEM should have min. 3 installation with similar system for Deep learning & Machine learning in different institutes (preferably in Education institutes, IITs, IISc, NIC, CSIR/DRDO/ISRO labs, large private players working in ML/DL etc.) with min. of 8 GPUs per node.	
		SI should have office in NCR & should have Engg. Certified on Deep learning (Profile of Engg. to be attached). SI must support in initial project once annotated data is available with institute in choosing the right model and train the model using popular opensource frameworks for a period of 1 year on-site. The topics for training should include the usage of GPU libraries/applications such as CUDA toolkit, CUDA tuned Neural Network (cuDNN), Primitives TensorRT Inference Engine, DeepStream SDK Video Analytics CUDA tuned BLAS, CUDA tuned Sparse Matrix Operations (cuSPARSE) Multi-GPU Communications (NCCL), Kubernetes TensorFlow , Caffe , PyTorch, Theano, Keras, caffe2, CNTK etc.	
		SI must provide 5 days training on system administration, Deep learning & Machine learning, Frameworks, Practical's with few popular modules & Inferencing.	

Technical specifications for Server (Node -9)			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
18	Chassis	2U or Higher Rack Mountable Chassis with 8 x 2.5" Bay	
	CPU	Server should be configure with 2 x Intel Xeon-Gold 6242 (2.8GHz/16-core/150W) Processor or better	
	Motherboard	Intel C621 Chipset or higher	
	Memory	Server should be configured with 4 x 128GB DDR4-2933 RAM or 16 x 32GB DDR4-2933 RAM. Server scalability should be up to 4TB & 48 DIMM slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	HDD Bays	Server to be populated with 4 x 960GB SSD (min. 3 DWPD) The drive carrier should have an automatic alert mechanism to avoid data-loss/downtime.	
	Controller	Server should support On board SATA software RAID controller supporting SSD/HDD PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB battery backed write cache (on board or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption	

	GPU	2 x GPU A100/40GB	
	Networking features	1 x Dual 10Gbe Base-T network adaptors with Management Port. 2 x singleslot InfiniBand HDR 100 GBps 2 x 1Gb Network port	
	Interfaces	Micro SD slot - 1/M.2 Drives with RAID1 4 Nos. of USB Ports with at least 2 USB 3.0	
	Power Supply	Server should have redundant 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply or equivalent power supply	
	Fans	Redundant hot-plug system fans	
	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support USB 2.0 Support Energy Star ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum)	
	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option Runtime Firmware Validation - Periodically scan essential firmware for compromised code during runtime	
	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware CentOS	
	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for	

		central management for enterprise-wide data encryption deployment.	
	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
	Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support RESTful API integration 8. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	
	Server Management	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port	

		3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support RESTful API integration 8. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	
		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware	
		The Systems Management software should provide Role-based access control	
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like Memory and HDD.	
		Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
		Availability of the firmware rollback feature in quoted server i.e. in case a wrong /malicious firmware up-grad happens on a server, have option to roll back to the last upgrade which was working fine.	

		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	
Technical specifications for Server (Node -10)			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
19	Chassis	2U or Higher Rack Mountable Chassis with 8 x 2.5" Bay	
	CPU	Server should be configure with 4 x Intel Xeon-Gold 6242 (2.8GHz/16-core/150W) Processor or better	
	Motherboard	Intel C621 Chipset or higher	
	Memory	Server should be configured with 4 x 128GB DDR4-2933 RAM or 16 x 32GB DDR4-2933 RAM. Server scalability should be up to 4TB & 48 DIMM slots.	
	Memory Protection	Advanced ECC with multi-bit error protection, online spare/spare-bank memory, mirrored memory and fast fault tolerance or Rank Sparing	
	HDD Bays	Server to be populated with 4 x 960GB SSD (min. 3 DWPD) The drive carrier should have an automatic alert mechanism to avoid data-loss/downtime.	
	Controller	Server should support On board SATA software RAID controller supporting SSD/HDD PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0, 1, 5, 6, 10, 50, 60 with 2GB battery backed write cache (on board or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption	
	Networking features	1 x Dual 10Gbe Base-T network adaptors with Management Port. 2 x singleslot InfiniBand HDR 100 GBps 2 x 1Gb Network port	
	Interfaces	Micro SD slot - 1/M.2 Drives with RAID1 4 Nos. of USB Ports with at least 2 USB 3.0	
	Power Supply	Server should have redundant 1600W Flex Slot Platinum Hot Plug Low Halogen Power Supply or equivalent power supply	
	Fans	Redundant hot-plug system fans	
	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support USB 2.0 Support Energy Star ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum)	

	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option Runtime Firmware Validation - Periodically scan essential firmware for compromised code during runtime	
	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware CentOS	
	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
	Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
	Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes	

		in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support RESTful API integration 8. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	
	Server Management	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Remote console sharing up to 4 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support RESTful API integration 8. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support	

		The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware	
		The Systems Management software should provide Role-based access control	
		Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
		Should help provide proactive notification of actual or impending component failure alerts on critical components like Memory and HDD.	
		Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
		Availability of the firmware rollback feature in quoted server i.e. in case a wrong /malicious firmware up-grad happens on a server, have option to roll back to the last upgrade which was working fine.	
		Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	
		The Server Management Software should be of the same brand as of the server supplier.	

Technical specifications for Storage (1 PB)			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
20	Eligibility Criteria	1) Entire storage solution must be from single OEM having L0, L1 & L2 support capability in India with support services. Single OEM must be able to support both file system and storage hardware by themselves up to fixing software bugs in file system and underlying RAID array, providing timely resolution. 2) Storage solution proposed must be certified to work with diverse computing architectures including X86-64 (Intel & AMD), NVIDIA GPU BASED SYSTEMS computing servers with GPGPUs. 3) Storage OEM must have deployed similar solutions in India. These sites must be under active support contract. Please submit proof of installation and customer contact details.	

	Capacity Requirement	Bidder to supply 1 PB raw capacity parallel file system storage solution in single global namespace such that it Should be configured with RAID 6 (8+2) or equivalent with dual parity Metadata capacity should be configured to accommodate at least two billion files.	
	Parallel File System	Latest version of OEM commercially supported IBM GPFS or OEM supported Lustre to be quoted	
	Storage Architecture	Storage solution must have: 1) Minimum two active-active controllers with redundant power supply and fans to prevent cache data loss during power failures. 2) Connectivity to computing cluster over RDMA capable 100Gbps HDR100 InfiniBand network 3) I/O servers and controllers must have redundant and highly available paths to computing cluster as well as backend disk enclosures. 5) Storage system must support global hot spares for NL-SAS / SSD disks. 6) The proposed storage system should tolerate simultaneous failure of any two disks is a single RAID group. 7) 20 TB or higher of the total usable capacity should be quoted as Meta data on SSD or SAS configured with RAID 1 or equivalent. 8) Solution should be balanced to manage failure (No Single point of Failure). 9) 1% of disk drives of PFS should be configured as hot online spare drives or capacity.	
	Standard File system Features	Storage solution must support: 1) User & Group Quota 2) POSIX compliance 3) Fine grained locking so that multiple clients can read & write from the same file simultaneously. 4) Ability to read and write in parallel to same file and different files. 5) Data striping across multiple I/O nodes and RAID LUNS. 6) Ability to transparently recover from client, server and network failures without losing data. 7) Ability to configure all capacity in single namespace as well as ability to create small namespaces. 8) Offered storage solution must be able to aggregate up to 8x 100 Gbps InfiniBand network connections from single computing server without needing to mount separate file system per network port. Proof of network aggregation with relevant benchmarks must be submitted. 9) Entire file system namespace must be mounted inside application containers without needing root/superuser privileges. 10) If any storage feature is licensed for capacity then, all licenses for entire capacity required to meet stated performance must be supplied.	

Connectivity	Disk Type storage should consist of NL-SAS/SAS 4 TB or higher capacity disks only. Storage solution must offer minimum 4 ports of RDMA capable 100Gbps InfiniBand ports (capable of operating with HDR InfiniBand specifications). Additionally, there must be minimum 1 port of 1Gbps Ethernet per storage controller for management and monitoring. Fast rebuilds: Storage must offer fast rebuild capability for replacing failed drives. Bidders must demonstrate rebuilding 10TB or higher capacity drive in less than 10 hours.	
Rebuild Performance	Bidders must demonstrate rebuild time of 10 hours of less for building single failed NL-SAS drive and rebuild time of 5 hours of less for building single failed SSD.	
Multi-tenancy & security	1) Storage solution must support multi-tenancy and security available in the propose File system should be deployed. 2) Storage solution must support security features to prevent untrusted clients for changing data via root squash. 3) Storage solution must provide audit logging facility to track actions on files & directories in the file system. At minimum, file system must support enabling audit logging on files/directory create, delete and renames. Any additional licenses required for all of above features must be supplied with appropriate bill of material in the tender response.	
High Availability & Redundancy	1)Entire storage solution must not have any single point of failure with high availability and redundancy offered at each layer of the I/O stack. 2) Entire Solution must be in balanced with respect to no. of I/O servers, network ports, backend connectivity etc. 3) Storage solution must have a minimum of two active controllers, hot swappable redundant power supplies and fans. 4) The proposed storage system should tolerate simultaneous failure of any two disks is a single RAID group.	
Single Pane of Glass monitoring	A single pane of glass monitoring solution must be offered with: - Ability to monitor file system and underlying storage arrays in same GUI dashboard. - Ability to show device health, performance, any alerts on a single dashboard - Ability to drill down on performance from clients, storage servers to controllers to disks - Ability to monitor storage usage for specific user or job in real-time.	
Scalability	Entire storage solution must support scale-out configurations up to 50 PB in single global namespace using similar building blocks.	
Aggregate Performance Requirements	1)To deliver minimum sustained write performance of 25 GB/s	

		2) Storage must also deliver aggregate IOPS performance of 1 Million random reads and 0.1 Million random writes with 4KB I/O size with benchmark tools and configuration mentioned below. 3) File creation capacity of minimum 80,000 files per second	
	Benchmarking tools	Bidder must submit benchmarking report along with tender response with: 1) Open-source IOR benchmarks (https://github.com/hpc/ior/releases) running on 8 compute nodes with 1 MB transfer size, and file size double than total storage cache and I/O node memory with -vv (double verbose) parameters and POSIX file per process workload are to be used for all throughput testing. 2) MDTEST Version 1.9.3 (https://sourceforge.net/projects/mdtest/files/mdtest%20latest/mdtest-1.9.3/) to be used for all metadata performance benchmarks running on 8 compute nodes with minimum parameters of "-n 100000 -i 3 -vv -w 4096 -u". 3) Bidder should submit the IOR benchmark for 50GB/s write performance and 50GB/s read performance with 1 MB block size and file size must be double than storage & I/O servers memory. Benchmarks must be run on minimum 8 and 16 compute nodes. Storage solution must deliver parallel file system metadata performance of minimum 60,000 files creates/sec. Bidders must also submit output of IOR and MDTEST. 4) Bidder (OEM) should run the benchmark on 20 node PFS clients over 100G EDR 5) Detailed benchmark report should be submitted along with the bid.	
	Misc.	Necessary cable and connectors as per solution requirement should be provided.	
		Bidder must provide peak power in KW, heat in BTU/Hr, weight in Kg and air flow in CFM for cooling of the storage solution.	
		The OEM will be responsible for Supply, installation, configuration, commissioning, testing, maintenance and support for both hardware and software during the warranty period.	
		The installation/ integration should be done by OEM engineers only. OEM should submit engineer's details such as engineer name, employee code, total years of experience in PFS, and number of PFS installations carried out by that particular engineer on their letter head. A copy of installation report must be enclosed with the technical bid.	
	Management & Monitoring	If the proposed storage system is composed of a number of external servers for various services, the storage management system software must be able to monitor and manage these servers, with at least centralized boot/shutdown capability. If additional software is required to manage these external servers, tenderers shall provide that software with enough licenses for the storage system. Please describe the functions and mechanisms of the required software.	

Technical specifications for Switches			
Infiniband (IB) Mellanox Quantum HDR Edge Switch			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
21	Switch Specifications	Switch architecture should be fixed form factor fitting 19" ETSI rack.	
		Switch should be pure Data Center class switches supporting latest DC technologies.	
		40-port Non-blocking Managed HDR InfiniBand Smart Switch in a 1U switch	
		Switch should support full bi-directional bandwidth per port.	
		Backward compatible to previous speeds	
		Switch should have internal redundant power supplies and fans from day one.	
		Should support 80 gold+ and energy star certified power supplies	
		Switch should support non-blocking wire speed performance on all ports	
		1+1 redundant & hot-swappable power	
		16Tb/s aggregate switch throughput	
		The switch should support latency less than 90ns port to port.	
		The system shall operate without degradation of performance between 0°c and 40°c	
		Should support features such as static routing, adaptive routing, congestion control and VL2VL mapping with enhanced VL mapping to enable modern topologies (SlimFly, Dragonfly+, Torus).	
		Should support 4x48K entry linear forwarding database	
		Should support 9 virtual lanes(8 data + 1 management)	
		Should be Compliant with IBTA 1.21 and 1.3.	
		Should support 256 to 4Kbyte MTU	
	Modules & Accessories	Switches should be provided with all the relevant mounting & connecting accessories. All necessary connecting cables and other accessories need to be provided along with switch.	
		Necessary connecting DAC cables, splitter cables and transceivers supporting and other associated accessories to be considered as part of solution & must be provided along with switches.	

10G /100G Open Ethernet Switch			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
22		Shall be 1 RU, 19" Rack Mountable	
		Switch should have minimum 48 x RJ-45 Copper,10GBASE-Ts with6 x 40GbE uplinks	
		Switch should support 6 x QSFP each port supporting 40GbE or 4 x 10GbE with breakout cable.	
		Switch should support hot-swappable redundant power supply with 4+1 redundant fan modules.	
		Switch shall have Switching Capacity of 720 Gbps and forwarding rate of 1 Bpps.	

		Switch should support latency less than 720ns or platform supports 1000 ns again depends on packet size	
		Should support min 8 GB NAND flash, 8 GB RAM as system memory.	
		Should support buffer memory of 16MB per switch	
		Shall have minimum 16K MAC Addresses.	
		Shall have minimum 1000 Active VLANs and 4,000 VLAN Ids support	
		Should support STP, RSTP, PVST, and PVRST modes.	
		Should support MLAg/vPC.	
		Should support VRR or VRRP.	
		Should support IGMP and MLD snooping.	
		Shall have 802.1p class of service, IP differentiated service code point (DSCP).	
		Supports static and dynamic routing protocols(OSPF/OSPFv3/BGP)	
		Switch should support hybrid cloud connectivity with QinQ and VXLAN tunnels.	
		Supports PortAdminEdge and BPDU guard feature.	
		Should support 802.1x authentication and accounting with Dynamic VLAN assignment.	
		Switch should support IPv4 and IPv6 ACLs.	
		Configuration and management through the CLI, GUI, console, Telnet and SSH	
		Supports SNMPv2/3	
		Network Time Protocol(NTP) or equivalent support	
		supports LDAP authentication, TACACS+, and RADIUS AAA.	
		Switch should support software upgrades via TFTP or FTP	
		IEEE 802.1 ab Link Layer Discovery Protocol (LLDP) support	
		Link Aggregation Control Protocol (LACP)	
		Switch should be IPv6 Certified/IPv6 logo ready/IPv6 ready	
		should be ROHS-6 compliant	
	Accessories & Support	Switches should be provided with all the relevant mounting & connecting accessories. All necessary connecting cables and other accessories need to be provided	
		Necessary connecting cables and transceivers supporting 10/40G and other associated accessories to be considered as part of solution & must be provided along with switches.	

Management Switch			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
23		Shall be 1 RU, 19" Rack Mountable	
		Switch should have minimum 24 nos. 10/100/1000 Base-T ports with additional 2 nos.1/10 gig SFP uplink ports	
		Switch should support 2 redundant, hot-swappable AC PSUs.	

		Should support 1 x RJ-45 serial console, 1 x RJ-45 100/1000BASE-T management port.	
		Switch shall have minimum 80 Gbps of switching fabric and 95 Mpps of forwarding rate.	
		Shall have minimum 16K MAC Addresses.	
		Shall have minimum 1000 Active VLANs and 4,000 VLAN Ids support	
		Should support STP, RSTP, PVST, and PVRST modes.	
		Should support MLAg/vPC.	
		Should support VRR or VRRP.	
		Should support IGMP and MLD snooping.	
		Shall have 802.1p class of service, IP differentiated service code point (DSCP).	
		Supports static and dynamic routing protocols(OSPF/OSPFv3/BGP)	
		Switch should support hybrid cloud connectivity with QinQ and VXLAN tunnels.	
		Supports PortAdminEdge and BPDU guard feature.	
		Should support 802.1x authentication and accounting with Dynamic VLAN assignment.	
		Switch should support IPv4 and IPv6 ACLs.	
		Configuration and management through the CLI, GUI, console, Telnet and SSH	
		Supports SNMPv2/3	
		Network Time Protocol(NTP) or equivalent support	
		supports LDAP authentication, TACACS+, and RADIUS AAA.	
		Switch should support software upgrades via TFTP or FTP	
		IEEE 802.1 ab Link Layer Discovery Protocol (LLDP) support	
		Link Aggregation Control Protocol (LACP)	
		Switch should be IPv6 Certified/IPv6 logo ready/IPv6 ready & should be ROHS-6 compliant.	
	Accessories & Support	Switches should be provided with all the relevant mounting & connecting accessories. All necessary connecting cables and other accessories need to be provided	
		Necessary connecting cables and transceivers supporting 10/40G and other associated accessories to be considered as part of solution & must be provided along with switches.	

Technical specifications of IP Based KVM Switch with display unit			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
24	Easy Operation	Three port selection methods: Manual (via front panel pushbuttons), Hotkey, and multi-language OSD (On Screen Display). Multi-language keyboard support includes US English, UK English, etc.	
	Auto Scanning and Broadcast Mode	Auto Scan provides hands-free monitoring of selected devices at changeable speeds. Broadcast Mode sends commands from the console to all computers – allowing you to perform operations	

		(such as software installations, upgrades, shutdowns, etc.), on all computers simultaneously	
	Superior Video Quality	Supports video resolutions up to 1920 x 1200 @ 60 Hz up to 30 meters, 1600 x 1200 @ 60 Hz up to 40 meters, and 1280 x 1024 @ 75 Hz up to 50 meters*	
	Multiple User Accounts	Supports up to 10 user and 1-administrator accounts. Two-Level password security – supports one administrator and ten user profiles. Password protection prevents unauthorized access to the installation Multiplatform support – Windows, Linux, Mac and Sun	
	Form Factor	One KVM console controls up to 8, 16, or 32 directly connected computers This space-saving innovation means that can be conveniently installed in a 1U system rack.	

ıl Specification for Firewall (Qty. - 1 nos.)

Model :

	Items	Descriptions	Compliance Yes / No
		Security Features	
25	General & Security Features	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	
		Firewall appliance should have at least 8 x 1GE RJ45 interface and 2 x 10G SFP+ interfaces	
		Firewall throughput should be at least 35 Gbps and it should have minimum 5Gbps VPN throughput	
		Firewall should support 2000 site-to-site & client to site VPN Tunnels	
		Firewall should support minimum 500 concurrent SSL VPN users and should be scalable in future. The OEM should provide VPN Client software for 500 users and should support various operating systems like Windows, Linux/Ubuntu and Mac	
		Firewall should support 5 Million concurrent sessions and 2,00,000 new sessions per second	
		The solution should support minimum 3.5 Gbps of NGFW (FW + IPS + AVC) throughput for Mix / production traffic	
		The solution should support minimum 3 Gbps of Threat Prevention (FW + IPS + AVC + AV) throughput for Mix / production traffic	
		Proposed Solution must support IPv6 and should have IPv4 to IPv6 transition. The proposed solution should be able to cater the clients/systems connected with IPv4 after the migration of NGFW to IPv6	

		The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode	
		The proposed system should have integrated Traffic Shaping functionality	
		The proposed system should support: IPSEC VPN, PPTP VPN and L2TP VPN	
		The device shall utilize inbuilt hardware VPN acceleration: (a) IPSEC (DES, 3DES, AES) encryption/decryption and (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 should support site-to-site VPN configurations with Route/Policy based IPSec tunnel	
		The system shall support IPSEC site-to-site VPN and remote user VPN	
		The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN	
		Intrusion Prevention System	
		NSS recommendation for complete device or IPS cabability	
		IPS throughput should be minimum 4 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 a configurable actions 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	
		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 solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole 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	
		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	
		High Availability	
		The proposed system shall have the capability for high availability (HA) features if required in future	
		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	
		Should have dedicated hardware/virtual appliance/client software for logging and reporting solution along with required-licenses	
		Real-time display of information for analyzing real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic	
		The firewalls management system shall support the option of exporting logs in CSV/XLS, XML and syslog and also capable of export into PDF	
		The firewall management system shall support real-time log forwarding in syslog and CSV formats	
		The firewall management system should support sending of customized usage & performance reports through mail at defined schedules such as daily, weekly, monthly or predefined time	
		The firewall shall offer inbuilt management feature through https, SSH, CLI etc. or centralized management with integrated log server. At RCB, 1 no. firewall will be installed in NON-HA mode.	
		The firewalls management system shall support detection and notification of performance degradation such as critically high CPU and memory utilization and when maximum supported number of concurrent sessions reached	
		The firewall should have hot swappable redundant power supply units	

Technical specifications for Workstation			
Make & Model :			
Sr.No	**Items**	**Descriptions**	**Compliance Yes / No**
26	Processor	Intel i7-9th Gen. or Higher	
	Memory	32GB (2x16GB) DDR4 2666, System should support Max. 128GB DDR4-2666 4 DIMM slots.	
	HDD	1 x 512GB SSD, 1 x 1TB 7200RPM SATA	
	Graphic Card	NVIDIA Quadro P400 2GB	
	Operating Software	Windows 10 Pro. (64 bit)	
	I/O Ports	Front : 1 headphone/microphone combo; 2 USB 3.0, 1 USB 3.1 Type-C Rear : 1 audio-in; 1 audio-out; 1 RJ-45; 2 DisplayPort 1.2; 2 USB 2.0; 4 USB 3.0	
	Expansion Slots	1 PCIe 3 x4 (x16 connector); 2 M.2 PCIe 3 x4; 2 PCIe ports 1 PCIe Gen 3 x16; 2 PCIe 2 x1 (x4 open ended connector)	
	Power Supply	500W wide-ranging, active Power Factor Correction, 90% Efficiency or equivalent	
	Keyboard & Mouse	USB KB & Mouse	
	Monitor	24"	

27	REDHAT	REDHAT Linux Standard	

25. HPC CLUSTER MANAGEMENT SOFTWARE

25.1 OEM supported or managed by OEM or equivalent features Cluster Management Software (CMS) suit should be offered for provisioning and managing all the compute nodes in the Cluster.

25.2 CMS is required to manage the complete cluster. It should have the ability to verify and ensure consistency in hardware and system settings across the Cluster's resources from a single console. CMS must support the following:

I. It must be a GUI/Web-based tool accessible from any client.

II. Must be user friendly to manage

III. It should provide a single interface for management and control of the complete cluster.

IV. It should provide the facility to dynamically add, remove or configure any individual node.

V. It should provide for remote booting/resetting of individual or group of nodes.

VI. It should provide for monitoring of vital parameters managing as many different images as needed for different software stacks, different operating systems, or different hardware.

VII. Cloning from one to many nodes at a time with a scalable algorithm which is reliable and does not stop the entire cloning process if any nodes are broken.

VIII. Replicating available images on any number of compute nodes in the cluster.

IX. Customizing reconfiguration scripts associated with each image to execute specific tasks on compute nodes after cloning.

26.OPERATING SYSTEM

1. Latest RHEL for all nodes. In case external storage IO nodes are offered in the solution, necessary RHEL licenses or OEM based OS for IO nodes to be included.
2. All Software quoted must be licensed, perpetual in nature with 5-years support (Initial 3 years support + 2 years during extended warranty) for updates / upgrades.
3. All necessary software device drivers should be provided.
4. All necessary cables, cable managers, cable guides if needed for structured cabling to be supplied.

27.WORKLOAD MANAGEMENT SOFTWARE

1. OEM supported or managed by OEM or equivalent features for all nodes with warranty upgrade.
2. Integrated advanced scheduling features should include cross-system scheduling, peer-to-peer scheduling with advanced fair share & hierarchical fair share scheduling, multi-cluster scheduling.
3. Power aware job scheduling to support auto shutdown and auto boot of nodes as per the workload to be supported with minimum delay.
4. The PBS works suite should have PBS Access & PBS Control with GUI Job Submission, monitoring, Analytics and Remote visualizations and PBS professional with required licenses or equivalent OEM supported.
5. PBS Access i.e. PBS Works for web-based job submission, management and monitoring or equivalent OEM supported. (Minimum 5 users concurrent users or higher).

Software Stack: All the software quoted must be licensed and perpetual.

28. ADMIN / CONSOLE NETWORK /MANAGEMENT

1. Admin and Console Network should be on different physical switches and should not be clubbed in the Primary Interconnect Enclosure or Switch.
2. All nodes need to be connected by Gigabit network for remote management hardware as well as for system network.
3. Managed GigE L2 Switches should be offered with suitable number of cables for Admin and Console Network.
4. Quantity of switches and cables and other required accessories to be provided as per proposed solution requirement.
5. Advanced license for IPMI based management and monitoring of all nodes.

29. SPECIAL TERMS & CONDITIONS AND COMPLIANCE TO BE SUBMITTED

1. The successful bidder, hereinafter called as System Integrator or 'SI', will be solely responsible for the upkeep of the GPU during the 1st three year of standard warranty as well as for two-year additional warranty.
2. The solution given for ML/DL workload should be certified by the respective OEM vendor to act as verified, tightly coupled architecture. Public document for the same should be available. The entire supporting document for the same should be submitted along with bid.
3. The solution should have ready to use container for different Big-data, ML, DL stack optimized for given architecture and configured to utilize GPUs fully.
4. The solution should be supported for 5 years including all spare parts, software stack, DL frameworks and contract for the same should be with OEM directly.
5. During the warranty, all the updates and upgrades for software should be given for free.
6. The solution provided should be highly scalable and should have reference architecture available for testing.
7. SI must provide 5 days training on system administration, Deep learning & Machine learning, Frameworks, Practical's with few popular modules & Inferencing.
8. Bidder must quote for all the requirements together viz HPC cluster, storage and Interconnect for the proposed solution. Partial response to the tender will be rejected.
9. The server, chassis management and monitoring software must be from the OEM itself.
10. The proposal must include
    a. Detailed data sheets for all the proposed component should be provided by the OEM/bidder
    b. The power and cooling requirement with supporting documents

c. Complete Bill of Materiel (BOM).

11. The warranty and support of the total solution shall commence from the date of final acceptance test and sign off on an acceptance report.

30. INSTALLATION AND SUPPORT

1. The OEM should do the integration/installation of the cluster at site.
2. During the warranty period, OEM will have to undertake comprehensive maintenance of the entire hardware and its components.
3. HPC cluster implementation should be monitored by a dedicated project manager of the bidder for smooth implementation.
4. OEM should provide onsite support during maintenance window such as DC shutdown, power outage and firmware upgrade.
5. Installation/configuration and upgradation of HPC cluster activities should be carried out by direct OEM engineers only.
6. HPL ratings (peak & sustained) for entire cluster configuration should be demonstrated after installation at site. Sustained HPL efficiency of the installed solution should be more than 60% of the offered theoretical peak performance.
7. The OEM should give 2-days System Administration training to a group of RCB & NIC personnel on installed hardware (Compute/storage/interconnect), operating system, installed system software and development tools including API. The training must be arranged at RCB & NIC offices.
8. Documentations should be submitted for the following:
    - Procedure for bringing up and shutting down the fully integrated cluster.
    - Procedure for user Creation/Deletion/Modification.
        - Procedure to get user accounting for Storage and Compute nodes.
        - Disk, health status monitoring of Master/IO nodes and storage enclosure.
        - Procedure for basic troubleshooting of Compute nodes, Storage & Head nodes (i.e. the installed applications on the Head nodes).
        - Step by step installation guide for the entire HPC implementation/configuration from scratch.
        - Project documentation listing hardware/software with serial numbers, configuration and connectivity.
        - Any other document/manual useful for daily administration.

ANNEXURE-I

CHECKLIST FOR SUBMISSION OF TECHNICAL PROPOSAL &COMPLIANCE

S.No	Item of Work	Proposed Make/model	Offered Specification w.r.t. Tender	Supporting documents Submitted along with part code (Catalogue/drawing /brochure)
	NIC Bhubaneswar			
1	Node-1			
2	Node-2			
3	Node-3			
4	Node-4			
5	Node-5			
6	Node-6			
7	Tape Library			
8	Storage			
9	Backup Software			
10	InfiniBand Switches			
11	10G Ethernet LAN Switches			
12	Management Switches			
13	KVM Switch with display unit			
14	Firewall			
15	Software to Build fully Functional HPC Cluster: - RHEL Master Node License - RHEL Compute Node License - Cluster Manager - Job Scheduler - Intel Compiler 2 user license			
	RCB, Faridabad			
16	Node-7			
17	Node-8			
18	Node-9			
19	Node-10			
20	Storage			
21	InfiniBand Switches			
22	10G Ethernet LAN Switches			
23	Management Switches			
24	KVM Switch with display unit			
25	Firewall			

26	Software to Build fully Functional HPC Cluster: - RHEL Master Node License - RHEL Compute Node License - Cluster Manager - Job Scheduler - Intel Compiler 2 user license			
27	Red Hat Ent. Linux (Std. Support)			
28	Workstation			
	7 nos Smart rack system, Physical Infrastructure (power, precision air conditioning, fire suppression, smoke detection, water leak detection, humidity sensor, intelligent monitoring system, security devices, setup of LAN points for 50 no. workstations etc.) Bidder must quote the all equipments, which are mentioned under data centre site.			

Signature & Seal of Bidder

ANNEXURE-II

TECHNICAL BID

Certificates/Documents to be submitted in the Technical Bid.

Note: If these documents are not submitted /conditions not met, the quotation shall be summarily rejected and no further correspondence, in this regard, shall be entertained.

S. No	Description	Technical Compliance (Yes/No)
1	Undertaking for adherence of Two-Bid System. (Non violation of Two-Bid System)	
2	Clarification with regard to manufacturer or their accredited agent.	
3	Undertaking for the submission EMD / Bid amount along with the bid.	
4	GST registration certificate	
5	PAN Card	
6	Fall clause declaration	
7	Non-black listing declaration	
8	Declaration reg. Proprietorship/partnership/ Pvt. Limited firm	
9	Samples and their test reports, wherever, applicable or decided by NIC or RCB	
10	Statement of financial standing from C.A. the last 3 years along with solvency certificate from Bank with address & proof of average turnover of the firm min. Rupees 1350.00 Lakh (In INR) for the last 3 years	
11	Different quality samples, if submitted, for one item, that particular item will not be considered for evaluation.	
12	Undertaking for adherence & acceptance to all Tender Terms as per Schedule – 'A' (No Deviation of Tender Terms)	
13	The Firm/office/service Centre in Delhi-NCR (Address proof)	
14	Certificate/Declaration for tender (Annexure-XVII)	

ANNEXURE-III

PROFORMA OF PRICE BID

The rates to be quoted online for each item of the Price Bid/BOQ in Indian Rupees, both in figures and words for the execution of work on 'Turnkey Basis' including all the required material, labour, accessories, tools & tackles etc., taxes, duties & levies for the complete work, as per Scope of Work, Specifications and approved design & drawings. The Price Schedule with rates and amount duly filled in and shall be uploaded in the desire format, as given in Instructions to Bidder.

S.No	Item of Work/Description	Unit	Qty.	Rate per unit	Applicable Taxes in %	Tax Amount	Total amount (with Tax)
	NIC Bhubaneswar						
1	Node-1	No's	3				
2	Node-2	No's	2				
3	Node-3	No's	2				
4	Node-4	No's	6				
5	Node-5	No's	4				
6	Node-6	No's	12				
7	Tape Library	No's	1				
8	Storage	No's	1				
9	Backup Software	No's	1				
10	InfiniBand Switches	No's	1				
11	10G Ethernet LAN Switches	No's	2				
12	Management Switches	No's	2				
13	KVM Switch with display unit	No's	2				
14	Firewall	No's	2				
15	Software to Build fully Functional HPC Cluster: - RHEL Master Node License - RHEL Compute Node License - Cluster Manager - Job Scheduler - Intel Compiler 2 user license	bundled	1				
	RCB, Faridabad						
16	Node-7	No's	1				
17	Node-8	No's	4				
18	Node-9	No's	6				
19	Node-10	No's	2				
20	Storage	No's	1				

21	InfiniBand Switches	No's	1				
22	10G Ethernet LAN Switches	No's	2				
23	Management Switches	No's	2				
24	KVM Switch with display unit	No's	2				
25	Firewall	No's	1				
26	Software to Build fully Functional HPC Cluster: - RHEL Master Node License - RHEL Compute Node License - Cluster Manager - Job Scheduler - Intel Compiler 2 user license	bundled	1				
27	Red Hat Ent. Linux (Std. Support)	No's	0				
28	Workstation	No's	35				
29	7 nos Smart rack system, Physical Infrastructure (power, precision air conditioning, fire suppression, smoke detection, water leak detection, humidity sensor, intelligent monitoring system, security devices, setup of LAN points for 50 no. workstations etc.) Bidder must quote the all equipments, which are mentioned under data centre site.	Lump Sum					
30	Additional warranty for 2 years after completion of 3 year standard warranty for NIC Bhubaneswar	No's	1				
31	Additional warranty for 2 years after completion of 3 year standard warranty for RCB Faridabad	No's	1				
	TOTAL (A) in Figures Rupees						
	TOTAL (A) in Words Rupees						

ANNEXURE-IV

APPLICATION FORM

[NOTE: On the letterhead of the applicant including full postal address, email address, telephone no. and fax no.]

Date: _____

To,

The Executive Director,

Regional Centre for Biotechnology NCR Biotech Science Cluster,

3rd Milestone Faridabad– Gurgaon Expressway,

Faridabad 121001.

Sir/Madam,

1. Being duly authorized to represent and act on behalf of ……. (hereinafter referred to as "the Applicant") and having reviewed and fully understood all the pre- qualification information provided, the undersigned hereby applies to be pre-qualified by yourselves as a tenderer for award of work(s) Supply, Installation, Testing, and Commissioning (SITC) of Indian Biological Data Center (IBDC) at NIC Bhubaneswar Data Center and RCB, Faridabad on Turnkey Basis and its Day to-day operations

2. Being duly authorized to represent and act on behalf of ……. (hereinafter referred to as "the Applicant") and having reviewed and fully understood all the pre- qualification information provided, the undersigned hereby applies to be pre-qualified by yourselves as a tenderer for award of work(s) Supply, Installation, Testing, and Commissioning Supply, Installation, Testing, Commissioning (SITC) of Indian Biological Data Center (IBDC) at NIC Bhubaneswar Data Center and RCB, Faridabad on Turnkey Basis and its Day to-day operations

3. Attached to this letter are copies or original documents defining:
   (a) the applicant's legal status
   (b) the principal place of business
   (c) the place of incorporation (for applicants who are corporations) or the place of registration and the nationality of the owners (for applicants who are partnerships or individually owned firms)
   (d) Annexure no. I to XVI

4. Your agency and its authorized representatives are hereby authorized to conduct any inquiries or investigations to verify the statements, documents and information submitted in connection with this application, and to seek clarification from our bankers and clients regarding any financial and technical aspects. This letter of application will also serve as authorization to any individual or authorized representative or any institution referred to in the supporting information, to provide such information deemed necessary and requested by you to verify statements and information provided in this application, or with regard to the resources, experience, and competence of the Applicant.

5. Your agency and its authorized representatives may contact the following persons for further information on general, personnel, technical and financial enquiries.

Contact 1: Name, email and Phone no.

Contact 2: Name, email and phone no.

6. This application is made with the full understanding that:

(a) Bids submitted by applicants will be subject to verification of all information submitted at the time of bidding

(b) Your agency reserves the right to:

- amend the scope and value of the contract / bid under this project; in such event, bids will only be called from pre-qualified bidders who meet the revised requirements; and
- reject or accept any application, cancel the pre-qualification process, and reject all applications without assigning reasons or incurring any liability thereof; and

(c) Your agency shall not be liable for any such actions and shall be under no obligation to inform the applicant.

7. The undersigned declares that statements made and the information provided in the duly completed application are true and correct in every detail.

Signed and Sealed, Name ……..

For and on behalf of …….

ANNEXURE-V

GENERAL INFORMATIOM

Name of Firm	
Head office address	
Telephone	**Contact No**
Fax. No.	**Email ID**
Place of Incorporation registration	**Year of incorporation/registration**

Signature and seal of the Authorized Signatory of the bidder

ANNEXURE-VI

FINANCIAL CAPABILITY

Financial Year	**Annual Turn Over in Indian Rupees (or equivalent to Indian Rupees) as per Audited Balance Sheet**
2016-17	**₹**
2017-18	**₹**
2018-19	**₹**

NOTE: The above data is to be supported by audited balance sheets

1. Attach copies of audited balance sheets duly certified by the chartered accountant for all three years (**2016-17, 2017-18 & 2018-19**). Audited Balance sheet should mention the membership number of chartered accountant issued by ICAI along with full address.

2. Attach recent solvency certificate from bankers. The certificate should be not more than one-year- old from the date of submission of bid.

Signature and seal of the Authorized Signatory of the bidder

ANNEXURE-VII

(To be submitted on Company Letter Head)

AUTHORIZATION LETTER

We___(name of the bidder) hereby authorize Shri / Smt. _____name of the authorized person) to sign and submit the bid to RCB, Faridabad against their tender No.:_____

Date:

Shri / Smt.___(name) is also authorized to negotiate the terms and conditions pertaining to the said tender on behalf of M/s _____ (name of bidder). The specimen signature of Shri / Smt. (name) is appended below.

Specimen Signature: Name:

The undersigned is authorized to delegate the authority on behalf of M/s ____ (name of bidder), as stipulated above.

For_____ (name of bidder)

ANNEXURE-VIII

(To be submitted on Company Letter Head)

TENDER ACCEPTANCE LETTER

Date:_____

The Executive Director
Regional Centre for Biotechnology,
3rd Milestone, Faridabad – Gurugram Expressway, Faridabad – 121001

SUB: Acceptance of Terms & Conditions of Tender Reference No: _____

Name of Tender / Work: Supply, Installation, Testing, and Commissioning (SITC) of Indian Biological Data Center (IBDC) at NIC Bhubaneswar Data Center and RCB, Faridabad on Turnkey Basis and its Day to-day operations'

Dear Sir,

1. I/We have downloaded / obtained the tender document(s) for the above mentioned `Tender/Work' from the web site(s) namely: www.rcb.res.in, https://dbt.euniwizarde.com as per your NIT / advertisement, given in the above mentioned website(s).
2. I/We hereby certify that I / We have read the entire terms and conditions of the tender documents (including all documents like annexure(s), schedules(s), etc.), which form part of the contract agreement and I / we shall abide hereby by the terms / conditions/ clauses contained therein.
3. The corrigendum(s) issued from time to time by your department/organization too has also been taken into consideration, while submitting this acceptance letter.
4. I/We hereby unconditionally accept the tender conditions of above mentioned tender document(s)/corrigendum(s) in its totality/ entirety.
5. I/We do hereby declare that our Firm has not been blacklisted/ debarred by any Govt. Department/Public sector undertaking.
6. I/We certify that all information furnished by our Firm is true & correct and in the event that the information is found to be incorrect/untrue or found violated, then your department/organization shall without giving any notice or reason therefore or summarily reject the bidder terminate the contract, without prejudice to any other rights or remedy including the forfeiture of the fully said earnest money deposit absolutely.

Yours Faithfully,

Authorized signatory
(Signature of the Bidder, with Official Seal)

ANNEXURE-IX

Note: This letter of authority should be on the letterhead of the quoting firm and should be signed by a person competent and having the power of attorney to bind the same

FALL CLAUSE DECLARATION

Tender No.: _____ Date : _____

Name of Work: Supply, Installation, Testing, and Commissioning (SITC) of Indian Biological Data Center (IBDC) at NIC Bhubaneswar Data Center and RCB, Faridabad on Turnkey Basis and its Day to-day operations'

This is to certify that we have offered the maximum possible discount to you in our financial bid Dated_____

The prices charged for the stores supplied under this Contract should under no event be higher than lowest prices at which the party sells the items of identical description to any other Govt. organization/PSU's/Autonomous bodies/Pvt. Organizations during the period of contract failing which the "FALL CLAUSE" will be applicable.

In case, if the price charged by our firm is more, RCB Faridabad will have the right to recover the excess charged amount from the subsequent/unpaid bill of the supplier.

Seal and Signature of the Bidder

.

ANNEXURE-X

NON-BLACK LISTING DECLARATION

(Format of undertaking, to be furnished on Company letterhead with regard to blacklisting/ Non- Debarment by Organisation)

To,
Executive Director
Regional Centre for Biotechnology NCR Biotech Science Cluster,
3rd Milestone, Faridabad-Gurgaon Expressway, Faridabad

We hereby confirm and declare that we, M/s ----------, is not blacklisted/ De-registered/ debarred by any Government department/ Public Sector Undertaking/ Private Sector/ or any other agency for which we have Executed/ Undertaken the works/ Services during the last 5 years.

For ----------

Authorized Signatory

Date:

ANNEXURE-XI

EXPERIENCE OF COMPLETION OF PROJECTS OF SIMILAR NATURE & COMPLEXITY

(During last seven years ending last day of month previous to the one in which applications are invited)

Sl. No.	Name of work/project and location	Owner or sponsoring organization	Cost of work in Lacs	Date of commencement as per contract	Stipulated date of completion	Actual date of completion	Name and address/ telephone number of officer to whom reference maybe made	Remarks

NOTE: Please attach supporting documents (completion certificates along with order copies) for the above information

Signature and seal of the Authorized Signatory of the bidder.

ANNEXURE-XII

LITIGATION DETAILS (COURT CASES/ARBITRATION)

Year	Name of the work	Name of the client with address	Title of the court case/ Arbitration	Detail of the Court/ Arbitrator	Status pending/ decided	Dispute Amount (Current Value, the equivalent) in case of court cases/arbitration	Actual awarded amount (Rs.) in decided court case/ arbitration

Signature and seal of the Authorized Signatory of the bidder.

ANNEXURE-XIII

CERTIFICATE FOR SITE INSPECTION

Certified that we……. (Name of tenderer) have visited the site on dated……. and assessed the nature and amount of work involved before submitting our offer. We will be able to complete the works within the stipulated time and also certified that we will be able to supply the material/executing the work as per specification to suit the site conditions.

Addresses of the sites:

1. Regional Centre for Biotechnology,
   3rd Milestone, Faridabad-Gurugram Expressway,
   Faridabad 121001, Haryana.

2. NIC, Sachivalaya Marg, OSHB Ln,
   Opposite to, Bhauma Nagar,
   Bhubaneswar, Odisha 751001

Signature of Tenderer with Seal & Date

ANNEXURE-XIV

SCHEDULE OF CONTRACT

1.	Earnest Money to be deposited	**Rs. 90 Lac**
2.	Time of Completion	**Twenty Two Weeks** from the date of award of Contract
3.	Compensation for delay	**1.5% per month of the tender value of work to be calculated on per day basis.**
4.	Defect Liability Period	**12 months** from the date of completion and handing over of work.
5.	Terms of Payments	**As per tender documents.**
6.	Schedule of Payment	**As per tender documents.**

ANNEXURE-XV

FORM OF AGREEMENT

This Agreement made on the_day of _____20 between Regional Centre for Biotechnology (RCB), Faridabad-Haryana for entering into the work(s) Supply, Installation, Testing, Commissioning (SITC) of Indian Biological Data Center (IBDC) at NIC Bhubaneswar Data Center and RCB, Faridabad on Turnkey Basis and its Day to-day operations herein after called "The Employer") who enters into this Agreement of the one part and M/s _____ (hereinafter called "The Contractor") of the other part.

Whereas the Employer is desirous that certain works should be executed by the Contractor, viz _____("the Works") and has accepted a Bid by the Contractor for the execution and completion of the works and the remedying of any defects therein.

Now this Agreement witnessed as follows:

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

2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz:

   (a) The Letter of Award;

   (b) The said Bid;

   (c) The General Conditions of Contract;

   (d) Prequalification document

   (e) Instructions to Tenderers and Specific Conditions of Contract;

   (f) The Specification;

   (g) The Drawings;

   (h) The Priced Bid

   (i) Any other relevant documents referred to in this Agreement or in the aforementioned documents

3. In consideration of the payments to be made by the Employer to the Contractor as hereinafter mentioned, the Contractor hereby covenants with the Employer to execute and complete the Works and remedy any defects therein in conformity in all respects with

the provisions of this work.

4. The Employer hereby covenants to pay the Contractor in consideration of the execution and completion of the Works and the remedying of defects therein the Contract Price or only such other sums as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract

In Witness whereof the parties hereto have caused this Agreement to be executed the day and year first before written.

Signed, Sealed, and Delivered by the Said

Binding Signature for and on behalf of RCB-Faridabad Binding Signature of Contractor

In the presence of:-

Witness (1):

Witness (2):

ANNEXURE-XVI

SERVICE LEVEL AGREEMENT
(Acceptance of SLA to be submitted on Company Letter Head)

SEVERITY LEVEL	MAXIMUM PRIMARY RESPONSE TIME		RESOLUTION TIME (RESTORE OR WORK-AROUND)	REMARKS
Level 1- **Critical**	Hardware failure	30 Minutes	Within same Business Days	Onsite support may take the necessary measures and If not repaired, Replacement of the device should be provided by the vendor.
Level 2 – High	Configuration Issue	1 Hours	Within two Business Days	Onsite support
Level 3 - Moderate	Any New Configuration	4 Hours	Within three Business Days	Onsite support

ANNEXURE-XVII

CERTIFICATE / DECLARATION FOR TENDER

(IN COMPLIANCE WITH THE F. NO. 6/18/2019-PPD DATED 23RD JULY 2020 OF DEPARTMENT OF expenditure, MINISTRY OF FINANCE, GOVERNMENT OF INDIA)

I/We have read the clause regarding restrictions on procurement from a bidder of a country, which shares a land border with India. I/We certify that as a bidder, I/We are fulfilling the requirements/conditions mentioned in the OM no. F. No. 6/18/2019-PPD dated 23rd July 2020 of Department of Expenditure, Ministry of Finance, Government of India and not barred to be considered in the bid process.

Signature of Tenderer with Name, Designation, Seal & Date

ANNEXURE-XVIII

BANK GUARANTEE FORMAT

Whereas _____ (Name and address of the Bidder)
(here in after called the "Bidders")

has submitted its Bid dated _____ for the supply of _____
(here in after called the "Bid")

Against the purchaser's NIT No. _____
Know all persons by these presents that we _____
having our registered office at _____
(Hereinafter called the "Bank")
are bound unto RCB, Faridabad (here in after called the "Purchaser) in the sum of _____ for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this
_____day of _____ 20_____.

The conditions of this obligation are:

1) If the Bidder withdraws or amends, impairs or derogates from the bid in any respect within the period of validity of this Bid.

2) If the Bidder having been notified of the acceptance of his Bid by the Purchaser during the period of its validity:-

    a. If the bidder fails or refuses to furnish the performance security for the due performance of the Contract/Purchase Orders or
    b. If the bidder fails or refuses to accept/execute the Contract/Purchase Orders or
    c. If it comes to notice at any time, that the information/documents furnished in its Bid are false or incorrect or misleading or forged

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or more the three conditions, specifying the occurred condition(s).

This guarantee will remain in force up to_____(insert date of additional forty-five days after Bid validity) and any demand in respect thereof should reach the Bank not later than the above date.

…….
(Signature with date of the authorized officer of the Bank)
…….
(Name and designation of the Officer)

…….
…….
(Seal, name & address of the Bank and address of the Branch)