IMPLEMENTATION OF DATA CENTER

FOR

UNIVERSITY OF KERALA

REQUEST FOR PROPOSALS

THIRUVANANTHAPURAM

JANUARY 2013

TENDER NOTICE

Tender No. **Pl.A1/Ad.Misc/IC/KUPortal/12**   Date: 05-02-2013

Sealed competitive bids are invited from reputed IT Companies / Organizations for the implementation of a Data Center for University of Kerala.

Name of Work: Implementation of Data Center for University of Kerala.

 Application Fee : Rs. 2,250/- **(to be submitted along with Technical bid**)

The amount must be remitted by crossed DD drawn in favour of The Finance Officer, University of Kerala, payable at Thiruvananthapuram. Technical bids without the fee will be rejected.

Earnest Money Deposit: ₹ 100,000/- (₹ one lakh only)

(Earnest Money Deposit is to be submitted along with Financial bid only)

The amount must be remitted by crossed DD drawn in favour of The Finance Officer, University of Kerala, payable at Thiruvananthapuram only.

Date of publication of RFP document: **05**-02-2013
Last date and time for submission of Technical bids: 22-02-2013 5 PM
Date & time of opening of Technical bids: **23**-02-2013 11 AM

Date & time of presentation: Will be intimated to bidders found successful in Technical bid

Date & time of opening of financial bids: Will be intimated to bidders found successful in Technical bid.

REGISTRAR
University of Kerala
Palayam, Thiruvananthapuram – 34
Phone: 0471 2305631

A. SCOPE OF THE WORK

1. University of Kerala intends to set up a full-fledged tier 3 Data Center for conducting different online activities. University invites proposals from interested firms or organizations experienced in this work for setting up the same.

2. The selected bidder shall arrange to undertake all the necessary civil, electrical, plumbing and mechanical works including false ceiling, flooring, partitioning, installation of electrical components, cable laying and other necessary services to create the Non-IT/ Physical infrastructure at the DC site. Bidder can inspect site for assessing as-is condition.

3. The selected bidder shall procure supply and install all IT (active and passive) and Non-IT components. Installation shall mean to install, configure and integrate every component and subsystem component, required for the functioning of the Data centre

4. The Data Center shall be tested for the following parameters:

    a) Electrical Requirements

    b) Cooling & Environmental Control

    c) Smoke & Fire Detection, Prevention & Suppression requirements

    d) Surveillance & Physical Security

    e) LAN Passive Components

    f) IT Security

    g) Successful hosting/ collocation of at least one departmental application, etc.

    h) Training on Data Center infrastructure.

    i) ITIL v3 based Ticketing tool for incident, change, problem & configuration management

Generation of documents during design, installation, commissioning and training phases shall be mandatory and be made available to the Tendering Authority.

5. **Network Management Service:** The objective of this service is to ensure continuous operation and upkeep of the LAN & WAN infrastructure at the DC including all active and passive components. WAN link is available at two campuses of the University - one at Palayam campus and the other at Kariavattom campus. For overall functioning of the data centre, the selected bidder shall be responsible to coordinate the WAN link related issues. The service to be provided for Network Management during warranty period include

   a) Ensuring network service support is available for 24 x 7 as per the prescribed SLAs

   b) Attending to and resolving network failures and snags

   c) Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches etc.

   d) Configuration and backup of network devices including documentations.

   e) Provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers.

   f) Installation and re-installation of the network devices in the event of crash/ failures.

   g) Tuning of various parameters to optimize performance and to ensure industry standard QoS with customization is being delivered.

6. **Backup / Restore Services:**

   a) Set up a Backup of storage as per the defined policies.

   b) Monitoring, log maintenance and reporting of status on a regular basis during warranty period.

7. **Configuration/ Reconfiguration Management Services:** The complete configuration including reconfiguration at no cost (on demand) (in hardcopy & softcopy) of the following items installed at DC.

   a) Router

   b) Switches

c) UTM Appliance

d) Proxy Server and DNS

e) Authentications System

f) Any other equipment, hardware/software installed under the project.

g) ITIL V3 based Ticketing tool for SLA management

8. **Subcontracting:** The bidder in his technical document shall provide the list of services planned to be sub contracted. The bidder may use subcontractors for the work force deployment & supply of consumables as part of the scope. **Subcontractors shall not be entertained for any of the core activities of the project proposed in the RFP.** It is clarified that the bidder shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the sub-contractors. The bidder undertakes to indemnify the University or its nominated agencies from any claims on the grounds stated herein above.

B. INSTRUCTIONS TO BIDDERS

1. The tenderers are required to quote their lowest rates separately for (i) Hardware, software component (ii) Civil and electrical works (iii) Implementation, configuration and AMC charges.

2. For awarding the tender for work, the entire project will be considered as a single work. The tender will be awarded to the lowest quoted tenderer, taking the sums of all costs connected with the project. There will be no separate work divisions or separate awarding of works to different bidders.

3. Each propoal should be accompanied with a Bank Draft for ₹ 1,00,000/- (₹ One lakh only) as Earnest Money Deposit, drawn in favour of the Finance Officer, University of Kerala,Thiruvananthapuram payable at State Bank of Travancore, KU branch, Thiruvananthapuram or Chelan remitted to cash counter, University of Kerala. Cheques will not be accepted. This deposit will

be refunded to the unsuccessful tenderers on their written request, without interest, on finalization of award of contract.

4.   Proposals must reach the tendering authority on or before the last date and time specified. Late proposals will be rejected.

5.   Before commencing the work the successful bidder has to execute an agreement to successfully complete the project as per the time schedule.

C. GENERAL CONDITIONS

1.   The proposed data center must be set up at Computer Center building, University of Kerala, Palayam Campus

2.   The proposed data center must be setup as per the technical requirements provided.

3.   The existing servers and other function components at the present server room must be utilised for up the new Data center.

4.   The existing UPS units must be configured in redundancy mode and two different power paths must be made available in the DC room.

5.   Access to data center premises must be restricted and monitored using adequate access control systems with electronic logging and storage. Video monitoring with storage is to be provided.

6.   Suitable fire protection systems must be provided.

7.   Promising uptime must be ensured for data center environmental infrastructure.

8.   The existing LAN system in computer rooms must be upgraded to cat 6A structured cabling.

9.   A connectivity is present existing between two campuses provide a synchronised backup storage from Palayam and Kariavattom campuses.

10. OFC connectivity between buildings in the campus are existing, check its scope and functionality for data transmission. Replace some OFC components, if necessary

11. The University has the right to ask for clarifications and to conduct negotiations with any or all vendors.
12. The University has the right to disqualify any vendor if they fail to provide the necessary clarifications or documents.
13. The University has the right to make any changes in their requirements or to change any specifications, at any time.
14. Bidder should submit a separate proposal for the civil, mechanical and electrical works.
15. If any of the facilities provided by the vendor is not found acceptable to the University, the University has the complete right to reject the facilities without giving any compensation.
16. The University will release the payment to facilities set up by the vendor only after inspecting the facilities and satisfying that the work is done as per the requirements.
17. The vendor has to complete the work as per the time schedule proposed. The University has the right to claim compensation for the delay in completing the work as per schedule.
18. The selected bidder shall design the Data Center in line with minimum requirements as laid out in TIA 942 specifications for Tier 3 Data centre. The design should ensure an uptime of 99.99% on a quarterly basis.
19. Bidder can visit the site of the proposed data centre, if they required.
20. The University has the right to cancel the work order at any time without assigning any reason.
21. The decision of the University in all matters will be final.

D. REQUIREMENTS DETAILS

D1. Server room setting

1. The IT infrastructure must be Tier 3 complant.
2. A dedicated clear space of 3.5 M x 5.0 M must be made available as server room space, at the computer centre and the web-casting centre at Kariyavattom.

3. To achieve the above requirement, the existing separation must be rearranged.

4. Raised flow air distribution system for complete distributed airflow always, preventing the possibility of water contamination or leakage affecting server room equipment is to be provided. Raised floor using pedestals, bolted stringers made of steel bars must be provided. Floor tiles with point load capacity of approximately 400 Kg. (plain as well as perforated floor tiles) with top lamination must be provided. Pedestals must support the panles and achieve a height of nearly 650 mm in the DC hall from the true floor level. It shall be placed in grids. The design must conform speedy assembly and removal for relocation and maintenance. Pedestal base shall be permanently secured to position on the floor by glue and mechanical fastening. Pedestal assembly shall provide easy adjustment of levelling and panels. Pedestals must be built using galvanized steels of hexagonal shaped sections and fixed on stringers of size 525 x 30 x 25 x 0.8 mm thick to form grides of 600 x 600 mm. The pedestal must support an axial load of 1700 Kg UDL. Floor insulation using aluminium foil on true floor and false floor with rubber adhesives must be provided.

5. Suitable ceiling at a height of 10 feet from the raised finished platform to keep a low ambient temperature is to be provided. The false ceiling must be in baked polyester painted perforated metal panel ceiling system with high NRC-CAC values above 0.70 for noise absorption and transmission, light reflectance better than 0.6. The ceiling must be of 600x 600 mm grid tiles of pre coated aluminium 0.6 to 0.7 mm thickness in approved acrylic colour. Grid suspension systems with 15 mm wide T section flanges and cross tees must be used. Humidity and fire resistant capacity for ceiling material is required. The suspension system must be made up of hangers of galvanized steel 26x26x25x1.2 mm with adjustable clips.

6. Doors, windows and opening are to be sealed using plastic films, vapour retardant paint, vinyl flooring and wall covering.

7. The server room entrance and exit must be made accessible using Biometric access or proximity cards.

8. The server room must be provided with redundant active distribution paths from diverse power sources from UPS room using control devices.

9. Additional Power outlets using single phase industry standard 32 A rating must be provided. Single point disconnection facility must be available.

10. Upgrading the existing active power control devices and sockets at the UPS room to higher capacity is required.

11. Proper electrical earthing to devices as per ISI standards is to be provided.

12. Installing lighting system in DC room with energy efficient devices with single as well as individual control facility is to be provided.

13. Emergency lighting facility during main power failure is to be provided.

14. Fire detection and suppression system must be procured and properly installed (certified system with no human intervention)

15. Water leakage detection system and fire alarm are to be procured and installed (Certified system only)

16. Electronic rodent control system with operational ability of varied frequencies must be procured and installed.

17. Caging of open ventilators for protecting equipment from rodent attacks is to be provided at DC room and UPS room.

18. The vendor while submitting the proposal must specify any additional equipment / requirement needed for any facility.

19. The vendor must specify the specifications (make, capacity, type etc.) of each qualified item while submitting the proposal.

D2. Upgrading LAN/WAN infrastructure

1. Procuring and installing 42 U rack in the DC room

2. Installing and configuring servers, switches, firewall and other devices including software and hardware components for DC operation.

3. Upgrading the existing LAN in computer rooms to Cat 6A structured twisted pair 100 ohm copper cabling with patch points, RJ-45 connector terminators in the rack, clear labelling for every port at both ends of patch cords.

4. Extending the BSNL leased line link from the main building to the proposed data center for VPN facility and configuring for remote access to Kariavattom campus is to be done.

5. The existing optical fibre link of campus networking is to be extended to the newly installed rack at DC room and configuring it are to be done.

6. Optical fibre link connecting main building, Controller of Examination building and Computer Center must be established through underground multimode fibre optical cables (laid as per standard ISI specifications). The links at both ends must be properly terminated in suitable racks procured by vendor.

7. Configuring the remote server at Kariavattom campus for data access through the BSNL leased line is to be done.

8. The vendor must specify any other requirements for the complete DC operations.

E. ELIGIBILITY CRITERIA

1. Bidder should be a company registered in India under the Company Act or should be Public sector organisation. Furnish certificate of registration.

2. Bidder is preferably an ISO 9001 certification organisation. Copy of the ISO certificate needs to be furnished. If the bidder has some certifications in networking, WAN management, Security etc, will be an added advantage.

3. The bidder should guarantee support for the complete system (hardware and software) for the next 3 years commencing from the date of commissioning.

4. Any Government / Government agency / Banks / Financial Institutions in India should not have blacklist the Bidder during the last 5 years. Self-declaration to that effect should submit along with the technical bid.

5. The bidder should have experience in setting up data center for Govt. / PSUs/ Universities etc. within the last three years. Bidder should submit documentary evidence to support their claims.

6. An average turnover of at least 5.0 Crores per annum for the last 3 years, as per the audited accounts, must be achieved in the case of non-government bidders.

F. TECHNICAL REQUIREMENTS

1. The Technical Bid will comprise of a covering letter, documents / annexure as proof against minimum eligibility criteria, details of software development & maintenance facilities, responses to functional & hardware specifications, incremental IT infrastructure in general and undertaking (as given in RFP). In submitting additional information, please mark it as '**Supplemental**' to the required response. If the bidder wishes to propose additional services (or enhanced levels of services) beyond the scope of this RFP, the proposal must include a description of such services as a separate attachment to the proposal.

2. Bidder is expected to price all the items and services proposed in the Technical Proposal. Tendering authority may seek clarifications from the Bidder on the Technical Proposal. Any clarifications by the Bidder on the Technical Proposal should not have any commercial implications. The Commercial Proposal submitted by the Bidder should be inclusive of all the items in the technical proposal and

should incorporate all the clarifications provided by the Bidder on the technical proposal during the evaluation of the technical Proposal.

3. Technical approach, methodology and work plan are key components of the Technical Proposal.

4. Bidder shall present their Technical Proposal containing:

a) **Understanding of work scope:** This section shall contain a clear and concise understanding of project requirements along with activities to be performed and deliverables to be provided based on the scope of work.

b) **Technical Approach and Methodology:** In this part, applicants should explain their understanding of the objectives of the assignment, approach to the assignment, proposed solution, proposes technology methodologies for carrying out activities and obtaining the expected outputs, and the degree of detail of such output. Bidder should also explain the proposed methodologies and highlight the compatibility of those methodologies to the proposed approach and the needs of the project. Bidder shall also include the Risk management, Business continuity plan and Quality assurance plans, etc., as a part of Approach and Methodology.

c) **Work Plan:** In this part the applicant should propose the main activities of the assignment, their content and duration, phasing and interrelations, meetings, milestones (including interim approvals by the Client), and delivery dates of the reports/ documents. The proposed work plan should be consistent with the technical approach and methodology, showing understanding of the Scope of Work and ability to translate them into a feasible working plan. A list of the final documents, including reports to be delivered as final output, should be included here. The work plan should be consistent with the Work Schedule. Milestones, Deliverables, Meetings and presentations shall be clearly mentioned.

d) **Capacity building:** Bidder should submit a brief approach note on training of staff during implementation. Bidder should provide hands on training before requesting for acceptance and completion of

implementation. Training and manuals should be provided to all the users

e) **Approach for Project implementation**: Detailed approach for carrying out the project implementation along with the support and maintenance during the contract. Bidders should submit a detailed approach for implementation. Bidders need to give detailed approach how they would implement complete project with integration plan.

f) **Detailed specifications:** Bidder shall also give specifications of hardware/software to be procured. Bidder must also attach attested copies of the brochures from the OEM for the equipment that they would be providing as a part of the assignment.

g) **Company profile:** Details of the Point of Contact along with brief work profile of the Bidder as well as other partner firms including relevant experiences of executing similar projects. Bidder may include relevant case studies and attested copies of completion certificates from clients in support of the case studies.

h) **Comments,** if any, on the TOR to improve performance in carrying out the project. Innovativeness shall be appreciated, including workable suggestions that could improve the quality/ effectiveness of the assignment. In this regard, unless the applicant states otherwise, it shall be assumed by tendering authority that work (time and effort) required to implement any such improvements, are included in the inputs shown in the project plan.

i) **Other Information:** Any other information relevant to the solution as preferred by the bidder can also be placed in the document. No additions or modifications are allowed at a later stage.

G. TECHNICAL BID

1. Sets of Technical bids prepared in an eco-friendly manner (avoid plastic cover sheets and spiral binding) should be submitted in a sealed cover, for the purpose of technical evaluation by the technical committee. The cover sheet of the document shall state

"PROPOSAL FOR IMPLEMENTION OF DATA CENTER OF THE UNIVERSITY OF KERALA" submitted by <name of bidder firm>.

2. It shall be a brief report having the following sections:

   a. Content Page

   b. 1 page executive summary

   c. Overview of the agency or company - maximum 1 page

   d. Summary for meeting eligibility criteria (proof to be appended)

   e. Overview of the human, technical and other resources of the bidder in the field of Data center and server room setting activities (Client list and documentary evidence may be attached as appendix) Maximum 2 pages.

   f. Proposed solution for the present project along with a SWOT analysis (strength, weaknesses, threats and opportunities). This should be in such a way that the technical committee will be enabled to take a decision on the bidders competence according technical requirement and terms and conditions. The details must include

   a.i. layout of server room

   a.ii. Facilities provided in server room

   a.iii. Power supply paths with details of redundancy / backup

   a.iv. Precision air conditioning

   a.v. Raised platform of server room

   a.vi. Security access system

   a.vii. Extending BSNL link to DC

   a.viii. Extending OFC link in DC

   a.ix. structured cabling layout in computer rooms

   a.x. OFC link from DC to main building and CE building

   a.xi. Proposed time schedule - 1 page

   a.xii. Compliance statements for ELIGIBILITY CRITERIA and TECHNICAL REQUIREMENTS.

   a.xiii. Any other details - maximum 2 pages

a.xiv. Appendices: Certified true copies of (i) Certificate for Date of Incorporation/ Registration, (ii) Commencement of Business (iii) documentary evidence for prior experience (iii) EMD agreement (iv) Signed copy of the RFP (iv) any other material referred to in the proposal.

ELIGIBILITY CRITERIA

Sl. No	Criteria	Whether complied (Y/N)	Supporting documents enclosed	Remarks

TECHNICAL REQUIREMENTS

Sl. No	Criteria	Whether complied (Y/N)	Supporting documents enclosed	Remarks

F. FINANCIAL BID

Financial Bid will be collected only from those who are found successful in the Technical Evaluation by a committee constituted by the University

The Bidder shall quote price in clear terms. Break up is given in the format for Financial Bid. The rates quoted should be inclusive of VAT and all other taxes.

Part – A (Specification - Appendix A)

i. Hardware components	Rate in Rupees inclusive of all taxes, freight etc.
1. Servers	

2. Switches and Switching process	
3. VPN routers	
4. Firewall (UTM appliance)	
5. Storage Network Area	
6. 42 U Rack	
7. UPS with battery	
8. Server-line camera	
9. Access control system	
10.. . .	
ii. Software Components	
Licensed software for	
1. Software-Operating system	
2. Network monitoring and control	
3. Link monitoring facility to monitor the status of connecting links.	
4. Any other software essential for the DC must be specified by the vendor	
5. Vendor must provide a warranty of 3 years for all software and hardware item free of charge.	
6. . . .	

Part – B

	Rate in Rupees
i. Civil works ii. Electrical work	

Part - C

i. Implementation and configuration charge ii. AMC for three years Year 1	

Year 2	
Year 3	

Note: No other conditions or statements should be included in the financial bid. The above table should be used in bidder's letterhead and signed by authorized signatory. Lowest tender is calculated by adding Part A, Part B and Part C.

G. **EVALUATION OF BIDS**

The technical competency of bidders shall be evaluated by an expert committee, which shall have the following terms of reference.

1. To decide on the eligibility of the bidder.
2. To decide on admitting the experience.
3. To decide on the technical competence of the bidder in implementing the project.
4. To decide based on presentation and demonstration done by the bidder whether they are capable of providing feasible solution that meets the user requirements.

H. PAYMENT TERMS

All payments will be made only after the completion of the project, its inspection and successful commissioning. There will be no part or advance payments.

I. LEGAL CONDITIONS

The decision of the University in all matters will be final. Any disputes arising in any matters connected with this project must be dealt by a court of law within the jurisdiction of Thiruvananthapuram district, Kerala only.

Appendix A: Hardware Specification

(a) Server – 5 nos

Parameter	Specifications
Processor	Server should be quoted with Single 6 Core Processor Intel Xeon E5-2630 95W 2.3GHz
L3 Cache	15 MB
Chipset	Intel Chipset/ OEM Chipset / Or Equivalent
Memory	Server should be configured with 16 GB memory PC3L-10600 CL9 ECC DDR3 1333MHz LP RDIMMs
DIMM Slots	Server should support 24 DIMM Slots
Memory Property	DDR3 Registered Memory with Active Memory Protection
Hard Disk Drives	2* 300GB, 2.5in SFF 10K 6Gbps HS SAS HDD . Server should support up to 8 2.5" SAS/SATA hard disk or Solid state drives
RAID Controller	Integrated 6Gbps SAS hardware RAID 0, 1, 10 and 5. Raid controller should support on line Raid level migration, on line capacity expansion and data scrubbing as well. The server should be quoted with 512 MB Flash for RAID 5.
Optical Drive (Optional)	DVD-ROM
Graphics Controller	16MB DDR2-SDRAM
Gigabit Ethernet Ports	Integrated Two Gigabit Ethernet ports with full duplex / TCP/IP Offload Engine (TOE).
PCI Slots	2 PCIe slots
Blower	Server to be configured with Redundant and Hot Swappable Blowers
Redundant Power Supply	Server to be configured with Redundant Power Supplies
Fiber Channel	Server to be configured with 1 number of Dual Port 8Gbpps Fiber Channel Adapters.
Dimensions	Height: 43 mm (1.7 in), width: 429 mm (16.9 in), depth: 734 mm (28.9 in)
Form Factor	1U
Server Management	Server should support Management features as :
	Latest OS failure screen capture
	Graphical console redirection over LAN
	Support for IPMI v2.0 compliant management software
	SSL (Secure Socket Layer) and LDAP (Lightweight Directory Access Protocol) support
	Serial Over LAN
	Highly secure remote power on/off
	System reset control
	The server should be able to alert impending failures on maximum number of components. The components covered under alerting mechanism should at least

	include Processors, memory, PCIe slots, VRMs, power supplies, fans, hard disk drives
Server Management	Should be able to discover systems and other resources in a heterogeneous environment and Collect inventory data about hardware and software that is currently installed on systems
	Should be able to view and manage the status, problems and events for discovered systems
	Should be able to determine the health, compliance, and performance of managed systems by viewing detailed information about the problems by inspecting the event log
	Capable of automatically send the notifications for hardware events or when thresholds are exceeded
	Should have feature like update manager for detecting and viewing out-of-date systems and also get a notification when systems are in need of updates and which updates are needed. Download, distribute and install available and requisite updates
	Should e able to do the graphical remote control tools including VNC, RDP, and web-based remote control for AMM, ILO, IMM, and RSA
	Able to discover and Work with virtualized environments including. Microsoft Virtual Server, VMware, and Xen. Capable of viewing topology that shows the connections between physical and virtual resources
	Create automation plans based on events from virtual and physical resources and automation actions such as relocating a virtual server based on critical hardware alerts
	Ability to discover network devices and review network device inventory . Able to Monitor the health and status of network devices. View network device configuration settings, and apply templates to configure devices
	Management software should have upward integration with HP OpenView , Microsoft System Center Operations Manager , CA Unicenter , Tivoli Enterprise

(b)   **Web & Application Server – 1 nos.**

Technical Specification	
Processor / CPU	Latest 64 bit Server populated with 2 No. of Quad-Core processor, minimum 2.0 GHz clock speed or equivalent / subsequently better. The CPU should be of latest generation at the time of bidding i.e. Vendor should offer the highest clock speed and cache supported on the offered model with latest supported/ compatible server chipset. The Server should be scalable to 4 processors
Architecture	X86 /RISC / EPIC as per OEM architecture
Operating System	Should support Industry-led operating system platforms including Windows Enterprise Linux, and OS proposed by Bidder. Media and complete documentation for the system to be provided.
Main Memory	The system should be configured with minimum 64 GB RAM (ECC), scalable up-to 512 GB. Vendor should quote fastest available memory speed with the server being quoted.
Hard Disk	4X300 GB SAS 15K RPM SAS or better hot plug drives with RAID 1 with Disk Mirroring Features. Server Should have HDD bays for future scalability.
Industry Benchmark	Should have published benchmarks for TPC-c or SAP or SPEC available. If no published benchmark result for the offered server & processor is available then the performance offered by the server will be estimated by linear extrapolation of a published result on a higher server model or a lower server model (with the same processor).
	If the OEM does not have particular benchmark on a specified server, the OEM can use an Internal benchmark to build the correlation between a benchmark and the proposed Server. The same has to be given in the OEM's letterhead and signed by an authorized person
Clustering	Server should be configured to support for OS level clustering.
Network Interface	Dual port 10/100/1000 Mbps Ethernet Adapter, with no single point of failure
	2 No. dual ported 4 Gbps Fiber Channel Adapter with

SAN Switch – 1nos

Sr. No.	Description
Base fabric switch	Switch to support 24 ports having 8 ports activated
Optical transceivers	8 numbers of 8 Gbps SFP optical transceivers to be quoted
Cables	number of 5m Fiber Optic Cable LC-LC to be quoted

Network Core Switches -1 nos

Sr. No.	Description
A. Hardware Features	
Interface Options	Minimum 44*10/100/1000 T Ethernet Ports + 4*1G SFP Ports + 2 Expansion Slots. Expansion Slots should provide minimum 4 * 10G SFP+ Ports or higher. SFP+ Supported include SR, LR, ER SFP Supported include T, SX, LX 1 fixed mini USB console port for management
B. Redundancy	Switch should support both Redundant AC & DC power supplies and fans.
C. Latency	Latency upto 4.6 microseconds or lower
D. Performance	100% Line-Rate Performance, 480 Gbps (Full Duplex) Non-Blocking Switching throughput
E. Software Features	
Security	802.1x with VLAN assignment, Private VLAN edge
	RADIUS, TACACS+, Wire Speed Filtering
	Flexible ACL combinations—L2-L4 criteria
	Source and Destination MAC, IP, TCP/UDP Ports. SSH v1, v3
	HTTPS Secure BBI, MAC Address move notification
	SCP, Shift B Boot menu (Password Recovery/ Factory Default)
VLANs	Port-based VLAN, 4096 VLAN IDs supported
	1024 Active VLANs (802.1Q), 802.1x with Dynamic VLAN assignment
	Private VLAN Edge
Trunking	LACP, Static Trunks, Configurable Trunk Hash algorithm,
	Cross Stack Trunks, Trunk Hashing support (RTAG 7)
Spanning Tree	Multiple Spanning Tree (802.1s), Rapid Spanning Tree (802.1w)
	Fast Uplink Convergence, PVRST+
Quality of Service	QoS 802.1p, DSCP, Weighted Round Robin
	Metering, 4MB buffers for queuing
Routing Protocols	128 Static Routes, Layer 2/3 Static Routes
	RIP v1/v2, OSPF v3, BGP, IPv6

High Availability	Uplink Failure Detection, HotLinks or equivalent
	Virtual Router Redundancy support (VRRP), Layer 2 failover
Multicast	IGMP v1, v2, v3 Snooping with 2K IGMP groups Monitoring
	Port Mirroring, ACL-based mirroring, sFlow version 5
Virtualization	VMready VI API support
	Virtual switch stacking with up to minimum 6 switches
	vNIC MIB support for SNMP, Netboot
F. Management Features	
Clients	CLI, Browser-based client, SSH, or Telnet
Standard Protocols	SNMP v1, v2c, v3, RMON, Secondary NTP Support, Accept DHCP
	LLDP, 16K MAC Table, 9K Jumbo Frames, 802.3X Flow Control
G. Environmental Specifications	Temperature - Ambient operating: 0º C to +40º C
	Altitude - Operating 3,050 m (10,000 feet)
	Acoustic - Noise - Less than 65 dB
	Heat Dissipation - 520 BTU/hour
H. MTBF	195,000 hrs with ambient operating temperature of 40º C

SAN storage – 1nos

Specification	Description
Storage Technology	The storage should be based on 6Gbps end to end within enclosure. The storage should have dual controllers in active active more, redundant and hot pluggable PSUs, hot pluggable HDDs for reliability.
Chassis / Rack	2U, Rack mountable.
Storage Capacity	The storage should be quoted with 20TB usable capacity using 450 GB 15K rpm, 3.5 in drives
Host ports	The storage should support 6Gbps SAS host ports, 8Gbps FC host ports, 1GbE ports, and 10GbE ports.
Host interfaces	The storage should have 4 numbers of native SAS ports by default and shall have option for upgrading 8Gbps FC ports .
Scalability	The storage should be capable of scaling upto 160 drives with LFF / SFF drives.
Cache	The storage should have 1GB cache per controller and 2GB per storage system. The cache should support cache flush. Should support cache mirroring during write cache.
Power Backup	Battery backup with minimum 96 hours or cache de-staging should be supported.

Disk drives	Storage should support 300/450/600GB 15K RPM Drives, 300/600/900GB 10K RPM drives, 1/2/3 TB NL SAS Drives, 200/400 GB SSD. The storage should support intermixing of the drives.
Raid Support	The storage should support the industry standard raid levels - Raid 0, 1, 3, 5, 6, 1+0.
OS Support	Sun Solaris, Microsoft, HP UX, IBM AIX, RHEL, Oracle, Suse, Vmware, MAC.
Supported Features	The storage should support 256 point in time copies, 128 storage partitioning, and remote replication. The storage should support at least 64 hosts.

UPS - 5 KVA, ONLINE - 1nos

Spec No.	Particulars	Specifications
1	UPS brand	ISO certified
2	Phase	Single
3	Power factor	0.9 / Above
4	AH of battery	130 AH
5	Battery type	Tubular
6	Number of batteries	10 / above
7	Battery warranty	3 years
8	Technology used	IGBT
9	Nature of output	True sine wave
10	Backup time	2 to 3 Hrs
11	UPS warranty	3Years

VPN ROUTER -2 NOS

S/N	Specification
1	(a) 3 Integrated 10/100/1000 Ethernet ports with 1 port capable of RJ-45 or SFP connectivity (b) 1 service module slot (c) 4 Enhanced High-Speed WAN Interface Card (EHWIC) slots (d) 3 onboard digital signal processor slots (e) 1 internal service module slot for application services
2	**Security** (f) Embedded hardware-accelerated VPN encryption

S N	Features
	(g) Secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN, or Enhanced Easy VPN (h) Integrated threat control with Content Filtering (i) Identity management: Intelligently protecting endpoints using authentication, authorization, and accounting (AAA), and public key infrastructure
3	**Voice** (j) High-density packet voice DSP module, optimized for voice and video support (k) Standards-certified VoiceXML browser services (l) Unified Border Element capabilities (m) Unity Express voicemail support (n) Support for Communications Manager Express and Survivable Remote Site Telephony

FIREWALL -1 NO

S N	Features	Y/N	Remarks
1	The Firewall should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.		
2	Appliance should be rack mountable		
3	The Firewall should be ICSA Labs certified for ICSA 4.0, EAL 4 certified and OPSEC Certified		
4	The Firewall should support integration with any existing security infrastructure as per OPSEC standards		
5	The platform must use a hardened OS.		
6	The platform should use hardware that is optimized for firewall, IPSec		
7	Appliance should support for Active – Active connections. It should not depend upon any 3rd party alliance.		
8	Licensing should be a per device and not user/IP based (should support unlimited users)		
9	Firewall Architecture should be on multiple tiers (firewall module, logging & policy management server, and the GUI/WebUI Console)		
10	The communication between all the components of Firewall System (firewall module, logging & policy management server, and the GUI/WebUI Console) should be encrypted with SSL or PKI.		
12	The firewall should be supplied with the support for RIP v2, OSPF & BGP routing protocols		
13	The firewall should support the multicast traffic to pass through the firewall system		
14	The firewall should support the multicast protocols as a multicast host, by participating in DVMRP, IGMP and		

		PIM		
15		The firewall should support multicast tunnels		
16		The firewall system should have a provision to handle the bandwidth management, if the same is required in future		
17		The firewall system should have a provision of adding the SSL VPN functionality in future, if the same is required.		
18		Should support Data Leak Prevention in future.		
19		The Vendor should also have a Software based solution which can run all the functionalities as per the requirement on an Open Server		
20		Should have URL filtering functionality		
21		Vendor should have an open architecture and not a fixed architecture eg: ASIC etc which will provide extra flexibility for growth and add newer features and functions without changing the architecture, design		
22		Design should be able to utilize exponential increase in performance every 2 years by enabling multithreaded function and been able to leverage architectural benefit from multicore architecture by distributing load of various security functions among multiple cores		

Interface and Connectivity Requirements

S N	Features	Y/N	Remarks
1	The platform must be supplied with at least 8 nos. of 10/100/1000Mbps of fixed copper interfaces expandable upto 12 in future. Should have support for Fiber modules as well is mandatory		
2	The platform should support VLAN tagging (IEEE 802.1q)		
3	The firewall should support ISP link load sharing		
4	The firewall interfaces have to support the unnumbered IP address		

Technical Requirements

S N	Features	Y/N	Remarks
1	Stateful Inspection Firewall		
2	Integrated Multi site management		
3	Built in storage capacity of 250GB minimum for storing logs.		
4	Power Input of 100 – 230V (50-60Hz)		
5	The box should be capable of upgrading to new versions/products incase a new feature is released by the OEM.		
6	Blocks attacks such as DoS, port scanning,		

	IP/ICMP/TCP-related		
7	Encryption support of AES 128-256 bit, 3DES 56-168 bit		
8	Password, RADIUS, TACACS, X.509, SecurID authentication merthords		
9	Integrated certificate authority (X.509)		
10	Should support 200 plus protocols.		
11	Should support star & mesh topology for VPN usage		
12	Should support an integrated IPS		
13	IPS should be capable a software fail open functionality incase of firewall performance going down.		
14	Should support unlimited policies.		

Performance Requirements

S N	Features	Y /N	Remarks
1	The Firewall must support at least 1.2 million concurrent connections.		
2	The Firewall must support at least 50000 new sessions per second processing.		
3	The Firewall should support at least 9 Gbps of Firewall Throughput in the base system. Additional hardware modules must not be used to achieve the same.		
4	The appliance should support integrated IPS throughputs of at least 4 Gbps		
5	The unit must have a management module (built-in management) capable to manage multiple sites for centralized management during expansion.		
6	Proposed device should have at least 4GB RAM inbuilt		

Firewall Filtering Requirements

S N	Features	Y/N	Remarks
1	The Firewall should also support the standard Layer 3 mode of configuration with Interface IP's. It should be possible to protect the firewall policies from being compromised.		
2	The Firewall must provide state engine support for all common protocols		
3	The Firewall must provide NAT functionality, including dynamic and static NAT translations		
4	The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type		

5	The Firewall should be able to filter traffic even if the packets are fragmented.		
6	All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, mime, s/mime, Lotus Notes, MS-Exchange etc		
7	The Firewall should support authentication protocols like LDAP, RADIUS and have support for firewall passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.		
8	The Firewall should support database related filtering and should have support for Oracle, MS-SQL, and Oracle SQL-Net.		
9	The Firewall should provide advanced NAT capabilities, supporting all applications and services- including H.323 and SIP based applications		
10	Support for Filtering TCP based applications		
11	Support basic inspection by working as a proxy for HTTP, FTP & SMTP traffic		
12	Support for Filtering incoming and outgoing e-mail based on size and filters. Should support gateway antivirus		
13	Should support CLI & GUI based access to the firewall modules		
14	Local access to firewall modules should support role based access		
15	Local access to the firewall modules should support authentication protocols – RADIUS & TACACS+		
16	Firewall should have an integrated IPS capable of software fail open option on failure & over load to ensure firewall availability.		
17	Integrated IPS should support hybrid attack detection/prevention with multiple attack protections methods, like Protocol Anomaly, Signature-Based, Day-Zero Protection, etc		
18	Integrated IPS should protect setup against vulnerabilities in the applications of the protected systems by carrying out deep packet inspection		

Firewall Logging, Statistics and Reporting Requirements

S N	Features	Y/N	Remarks
1	The Firewall must be able to send log information to an external log server via an encrypted connection		
2	The Firewall administration software must provide a means of viewing, filtering and managing the log data		
3	The Firewall logs must contain information about the		

S N		Y/N	Remarks
	firewall policy rule that triggered the log		
4	The Firewall must provide at a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall		
5	Support to log in detail all connections which are blocked		
6	Support to log in detail all connections which go through the Firewall		
7	Provision to report all denied connections inbound		
8	Provision to report all denied connections outbound		
9	Provision to report all successful connections inbound		
10	Provision to report all successful connections outbound		
11	Provision to report traffic levels for inbound & outbound destinations		
12	Support to generate performance statistics on real-time basis		
13	Capability to produce reports which measure usage		

Intrusion Prevention System

S N	Features	Y/N	Remarks
1	Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related		
2	Blocks attacks such as DNS cache poisoning, FTP bounce, improper commands		
3	Signature-based, behavioral, and protocol anomaly		
4	IPS should be a integrated system with firewall		
5	IPS should have a option to run in by-pass mode if the CPU of the device increases above a threshold limit – Software bypass		
6	IPS should have option to configure country based blocking		
7	IPS should be Certified & Recommended by NSS Labs		
8	IPS must protect from any evasion attacks, TCP split handshake attacks etc.		

Administration/ Management Requirements

S N	Features	Y/N	Remarks
1	Dedicated, integrated management system and real-time logs system should be provided		
2	The firewall management system must be capable of pushing firewall security policies and configurations to individual or multiple firewalls through a secure, encrypted connection interfaces		

			Y/N	Remarks
3	The Firewall must provide simplified provisioning for addition of new firewalls where by a standard firewall policy could be pushed into the new firewall			
4	The Firewall administration station must provide a means for exporting the firewall rules set and configuration to a text file.			
5	Any changes or commands issued by an authenticated user should be logged to a database.			
6	The Firewall must send SNMP traps to Network Management Servers (NMS) in response to System failures.			
7	Automatic synchronization ability of rules on multiple firewalls and the management servers at DC & DR sites when used			
8	Provision to generate automatic mail alerts			
9	Provision to send alerts to multiple recipients			
10	The Firewall must not support any non-secure means of access to the Firewall.			
11	Support for role based administration of firewall			
12	Management module should support Role-based approval, Self-approval & Emergency bypass with password)			
13	Only approved policies can be installed & email notification on installation of policies should be supported			
14	Should be capable of comparing different policies installed verses new policy intended to apply.			
15	Management server should give a full view on all changes to objects and rules to generate an audit log for any forensic/ compliance needs.			

User Authentication Requirements

S N	Features	Y/N	Remarks
1	Support for user authentication at the firewall system for the different TCP/IP applications, like HTTP, SMTP, Telnet & SSH		
2	Support for integration with the RSA Secure ID as the strong user authentication mode		

User Identity and Application Control

S N	Features	Y/N	Remarks
1	Should have integrated Identity Control		
2	Should have integrated Application Control		
3	Should Support User, User group based Policies		

4	Should support User Machine awareness		
5	Time based polices		
6	Should support Clientless and agent less authentication		
7	Should have Captive portal authentication		
8	Identity agent based authentication		
9	Application Library should have at least 4500 applications		
10	Should support minimum 275,000 Application widgets		
11	Application based logs		
12	User based logs		
13	Should support user check based feature which would document user decision on he has to access an application		
14	Should support bandwidth allocation based on applications		
15	Should not use any agents to be installed for AD/LDAP query		

42U Rack – 1 nos

Description	Qty
DK-PS Frame, 600W x 2000H x 1000D,Top cover with 4 x cutout of Dia 112, 2 x cut-out of Dia 112 for cable entry. Bottom cover with 4 x cutout of Dia 112 for cable entry. All cutouts blanked with Plastic caps. 2 pairs, 42U 19" L type angle Front & Rear on 6 x punched section. Color: RAL 9005	1
Side Panel 2000H X 1000D Screw Fixed, unvented (RAL 9005)	1
Perforated door, 2000H x 600W, RAL 9005	2
230V.AC,90 cfm fan(pack of 4). Fully Wired	1
Castor Wheels With Brake (1No)	2
Castor Wheels Without Brake (1No)	2
Component Shelf 720mm Deep For 900/1000 Deep Server Rack RAL 9005	2
Keyboard Tray For Server Rack with Brackets for 500mm Depth RAL 9005 for 1000D Panel	1
1U 19" Horizontal cable Manager (Zinc blue plated)	2
5/15A Socket Strip 10Sockets Indicator switch with 2.5 Mtr Power chord with 16A plug Colour: RAL9005 finish (LC)	2