

# High Court of Jharkhand, Ranchi

Ref. No. 1113 /Accts.

Dated: 05-02-2016

The Court is going to digitize all its Case Records and establish eCourt Rooms. Hence sealed quotations are invited from reputed manufacturers/Dealers/Venders/Firms by 12.00 noon 15.02.2016 for purchase of following articles.

## Total Requirement

| <b>Hardware required for eCourt</b> | <b>Total Requirement</b> | <b>Specification</b>               |
|-------------------------------------|--------------------------|------------------------------------|
| <b>NAS Storage with HA</b>          | 02 Nos.                  | <b>As Detailed in Annexure - A</b> |
| <b>L2 Switch</b>                    | 02 Nos.                  | <b>As Detailed in Annexure - B</b> |
| <b>L3 Switch</b>                    | 02 Nos.                  | <b>As Detailed in Annexure - C</b> |
| <b>Firewall with HA</b>             | 01 No.                   | <b>As Detailed in Annexure - D</b> |
| <b>Integrated Rack</b>              | 01 No.                   | <b>As Detailed in Annexure - E</b> |

Any further details may be collected from the Establishment of the Court during 10:00 a.m. – 5:00 p.m. on working days.

Sealed quotations are to be submitted in the office of the undersigned within the specified time.

### **Note:-**

1. Price quoted must be inclusive of all taxes and installation charges.
2. Maximum time required for supply of articles must be specifically mentioned.
3. Configuration must be at par or on the higher side (as referred above).
4. Service reputation of manufacturers / Dealers / Distributors in the market will be given priority.
5. Specification of quoted articles must be quoted in details.

Enclosures: As above (07 Sheets)

Sd/ **Anil Kumar Choudhary**  
**Registrar General**  
**High Court of Jharkhand, Ranchi**

## Annexure – A

| Technical Specification of Network Attached Storage (NAS)-02 nos. |  |            |
|---|--|------------|
| Features  | Minimum Specification  | Compliance |
| Make Offered  | -  |            |
| Model Offered   | -  |            |
| Rack mount  | NAS Controller shall be rack mounted with HA   |            |
| Processor   | Dual Quad Core latest generation Intel Xeon 2.2 GHz or higher.   |            |
| Memory  | 32GB DDR3 RAM or higher  |            |
| Hard Drives   | Shall be supplied with minimum of 64 TB Raw Space using 4TB 6Gbps SAS 7.2K rpm MDL drives  |            |
| Storage expandability   | Shall have more than 256TB scalability using SATA / SAS drives by providing associated hardware whenever required.   |            |
| Network   | Min. 4 X 1Gbps auto sensing NICs ports and shall be further scalable to additional 4 numbers of 1Gbps or 2 numbers of 10Gbps Ethernet port.  |            |
| Connectivity  |  |            |
| Protocols support   | TCP/IP, ISCSI, FTP, Common Internet file system (CIFS), HTTP, HTTPS, NFS 4, WebDev etc.  |            |
| Fault Tolerance   | Offered NAS shall support Raid 0, Raid 1, Raid 1+0, Raid 5 and Raid 6 (including for additional disk enclosures). Raid controller shall have minimum of 1GB flash back write cache.  |            |
| Network Client Types Support                                      | Should support Windows 7, 8, Windows 2008, 2012, Linux etc.  |            |
| Manageability   | Advanced interface with following<br>1. Common interface for NAS management tasks like CIFS, NFS, Volume Management etc.<br>2. Remote management<br>3. Common interface for Multi NAS management from a single console.  |            |
| Operating System  | Microsoft Storage Server – 64 bit edition in redundant OS hard disk drives   |            |
| File screening and quota management                               | 1. Offered NAS shall have support for file screening so that administrator can ensure that users shall not be able to store unwanted files on offered NAS device.<br>2. Offered NAS shall have Quota management for both Volume and Directory.<br>3. Software for both File screening as well as Quata management shall be provided. |            |
| File Management   | 1. Shall have flexibility to expire or move files to different folder / Location / Volumes / drives on the basis of polices like day of creation / modification etc.   |            |
| SAN storage (iSCSI based)   | Integrated iSCSI for block access over LAN.  |            |
| Snapshots   | Point in time copies of data to guard against data corruption.   |            |
| Encryption and compression  | Shall have support for encryption and Compression. License for both shall be offered.  |            |
| Replication   | Shall be offered with replication License for Disaster recovery.   |            |
| Host Bus Adapter  | Dual port 8 Gbps FC HBA to connect tape Library directly to the NAS  |            |
| Power Supply & Fan  | Redundant  |            |
| Warranty Support  | Warranty Support for 3 Years should be provided by the OEM Engineer directly and a letter of confirmation on the same should be provided by the OEM along with the Bid.  |            |

## Annexure – B

| <b>Technical Specification</b>               |  |            |                    |
|--|--|------------|--------------------|
| <b>Layer 2 Stackable Gigabit Edge switch</b> |  |            |                    |
| General                                      | Descriptions   | Compliance | Remarks/Deviations |
| Device Type:                                 | Full Managed Stackable Switch with Gigabit ports   |            |                    |
| Ports Qty:                                   | 48 10/100/1000BASE-T auto-sensing Gigabit Ethernet switching ports; 2 SFP+( 1/10G) Ports for fiber media support; 2 Dedicated Stacking Ports supporting 64 Gbps ,  |            |                    |
| Redundant Power supply                       | Support for Redundant Power Supply   |            |                    |
| Transceivers                                 | should come loaded with 2x 10G SR SFP+ Transceiver   |            |                    |
| Interfaces supported                         | Sx, LX, 1000 Base t, 10G SR . 10G LR   |            |                    |
| <b>Memory</b>                                |  |            |                    |
| CPU Memory                                   | minimum 1GB  |            |                    |
| Flash Memory:                                | minimum 128 MB flash   |            |                    |
| <b>Performance</b>                           |  |            |                    |
| Switching Capacity                           | Minimum 200 Gbps   |            |                    |
| Switching Throughput                         | Minimum 150 Mpps   |            |                    |
| MAC Address Table Size                       | 32000 MAC addresses  |            |                    |
| 802.1Q Vlans                                 | 4000 802.1Q vlans  |            |                    |
| <b>Networking Features</b>                   |  |            |                    |
| Routing Protocol:                            | Static routing support , RIP V1, RIPV2   |            |                    |
| Communication Mode:                          | Half-duplex, full-duplex   |            |                    |
| Switching Protocol:                          | Ethernet   |            |                    |
| Status Indicators:                           | Link activity, Power LED   |            |                    |
| Vlans  | Should support Port, Voice Vlan, Private Vlan, GVRP  |            |                    |
| DHCP and DHCP relay                          | Should support DHCP , DHCP relay   |            |                    |
| Redundancy Protocols                         | Should support STP, RSTP, MSTP , MLAG/Equivalent   |            |                    |
| Qos  | Flow based Qos service, port based qos service, ACL Qos, Diff serv   |            |                    |
| <b>Security Features</b>                     |  |            |                    |
|  | Should support 802.1x and Guest vlans  |            |                    |
|  | Should support MAC based port security by number of MAC  |            |                    |
|  | Should support Packet filtering at L2/L4 with flow based classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN. |            |                    |
| <b>Management Function</b>                   |  |            |                    |
| Configuration                                | Should support CLI, WEB based, and SNMP v1/v2/v3 based managements   |            |                    |
|  | Should support Sflow or equivalent technologies  |            |                    |
|  | Should support management vlans and Port namings to each interfaces  |            |                    |
|  | Should support LLDP  |            |                    |
|  | Should support Dual configuration and system files   |            |                    |
|  | Should support management function like Ping, Telnet,  |            |                    |
| <b>Miscellaneous</b>                         |  |            |                    |
| Authentication Method:                       | Secure Shell (SSH), RADIUS, TACACS+  |            |                    |
| <b>Power</b>                                 |  |            |                    |
| Power Device:                                | Power supply AC  |            |                    |
| Voltage Required:                            | AC 110/240 V ( 50/60 Hz )  |            |                    |
| Certifications                               | FCC Class A, ROHS  |            |                    |
| Market Presence                              | The OEM should have presence on Gartner Data Centre Networking Report May 2015 in the Quadreant Leaders, challengers and Visionary Quadreant and all proposed ethernet switches to be from the same OEM.                   |            |                    |
| Warranty                                     | Should support required SLA and lifetime warranty  |            |                    |

## Annexure - C

### Technical Specification Layer 3 10G switch : 2nos

| General                     | Descriptions   | Compliance | Remarks/Deviations |
|-----------------------------|--|------------|--------------------|
| Device Type:                | Full Managed Layer 3 10 G Stackable Switch   |            |                    |
| Ports Qty:                  | 48 x 10GbE SFP+ auto-sensing (10Gb/1Gb) fixed ports, 2 x 40 G QSFP+ ports 1x hot swap expansion module bay, 2x redundant AC PSU included   |            |                    |
| Redundant Power supply      | Should Support Dual Internal Field Replaceable Hot Swappable Redundant AC Power Supply   |            |                    |
| Interfaces supported        | Sx, LX, 1000 Base T, 10G SR . 10G LR . Should come loaded with 12 x 10 G SR , 16x 1000 Base T SFP ,  |            |                    |
| 40 G Support                | 40 G QSFP+ support from day one , 1x 40 g QSFP+ cables 1m to be supplied with each Switch. Support for Maximum 4x 40 G QSFP+ for scalability   |            |                    |
| <b>Memory</b>               |  |            |                    |
| CPU Memory                  | minimum 2GB  |            |                    |
| Flash Memory:               | minimum 256 MB flash   |            |                    |
| <b>Performance</b>          |  |            |                    |
| Switching Capacity          | Minimum 1280Gbps   |            |                    |
| Switching Throughput        | Minimum 960 Mpps   |            |                    |
| MAC Address Table Size      | 128,000 MAC addresses  |            |                    |
| 802.1Q Vlans                | 4000 802.1Q vlans  |            |                    |
| <b>Networking Features</b>  |  |            |                    |
| Routing Protocol:           | Static routing support , RIP V1, RIPV2 , OSPF (V1, V2 andV3) , VRRP, VRF, BGP  |            |                    |
| Software Defined Networking | SDN support from day one   |            |                    |
| IPV6                        | IPV6 should be supported from day one  |            |                    |
| Switching Protocol:         | Ethernet   |            |                    |
| Status Indicators:          | Link activity, Power LED   |            |                    |
| Vlans                       | Should support Port, Voice Vlan, Private Vlan, GVRP  |            |                    |
| DHCP and DHCP relay         | Should support DHCP , DHCP relay   |            |                    |
| Redundancy Protocols        | Should support STP, RSTP, MSTP , MLAG/Equivalent   |            |                    |
| Qos                         | Flow based Qos service, port based qos service, ACL Qos, Diff serv   |            |                    |
| Data centre protocols       | support for DCB with Priority Flow Control (802.1Qbb), ETS (802.1Qaz), DCBx, iSCSI Support , Open Flow support for software Defined networking   |            |                    |
| <b>Security Features</b>    |  |            |                    |
|                             | Should support 802.1x and Guest vlans , Port Mirroring   |            |                    |
|                             | Should support MAC based port security by number of MAC  |            |                    |
|                             | Should support Packet filtering at L2/L4 with flow based classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN. |            |                    |
| <b>Management Function</b>  |  |            |                    |
| Configuration               | Should support CLI, WEB based, and SNMP v1/v2/v3 based managements   |            |                    |
|                             | Should support Sflow or equivalent technologies  |            |                    |
|                             | Should support management VLANS and Port namings to each interfaces  |            |                    |
|                             | Should support LLDP  |            |                    |
|                             | Should support Dual configuration and system files   |            |                    |
|                             | Should support management function like Ping, Telnet,  |            |                    |
| <b>Miscellaneous</b>        |  |            |                    |
| Authentication Method:      | Secure Shell (SSH), RADIUS, TACACS+  |            |                    |
| <b>Power</b>                |  |            |                    |
| Power Device:               | Power supply AC  |            |                    |
| Voltage Required:           | AC 110/240 V ( 50/60 Hz )  |            |                    |
| Certifications              | FCC Class A, ROHS  |            |                    |
| Market Presence             | The OEM should have presence on Gartner Data Centre Networking Report May 2015 in the Quadreant Leaders, challengers and Visionary Quadreant and all proposed Ethernet switches to be from the same OEM.                   |            |                    |

## Annexure – D

### Firewall with HA

| <b>Firewall with HA</b>  |   |
|--|---|
| <b>Description</b>   |   |
| UTM/Full DPI Firewall throughput shall be  | 3000 Mbps or better                     |
| IPS throughput should be   | 4500 Mbps or better                     |
| Minimum Antivirus throughput shall be  | 3500 Mbps or better                     |
| Minimum IMIX throughput shall be   | 4400 Mbps or better                     |
| Minimum Stateful Packet Inspection Concurrent firewall sessions/ connections   | 1 Million or better                     |
| Minimum new firewall sessions/connections per second   | 90k or more                             |
| <b>Hardware Requirements</b>   |   |
| MultiCore Networking Specific Core[s]  | 24 Cores                                |
| Memory [RAM]   | 8 GB                                    |
| Interfaces   | 8 x 1GbE, 8 x 1GbE SFP & 4 x 10GbE SFP+ |
| Appliance Form Factor  | 1U RM                                   |
| Storage  | Flash Based                             |
| Power Supply & Fans  | Redundant & HotSwapable                 |
| <b>Warranty</b>  |   |
| 3 Years of Service, Subscriptions & 24x7 Support with advanced replacement warranty  |   |
| Item Description   | Requirement                             |
| <b>General Technical Specification – UTM</b>   |   |
| <ol style="list-style-type: none"> <li>1. The UTM should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general purpose operating systems.</li> <li>2. Appliance should have hardware/software acceleration so that processing is not slowed down by IPSEC/SSL VPN and content Inspection.</li> <li>3. UTM Appliance should have minimum space to store the firmware image and the UTM policies and AntiVirus + IPS signatures.</li> <li>4. UTM Appliance with Unrestricted users.</li> <li>5. Should have upgradeable Firmware</li> <li>6. Should Have a Re-Assembly Free Deep Packet Inspection or equivalent feature</li> <li>7. Gateway Antivirus should be able to scan the 50+ Protocols including HTTP, FTP, SMTP, POP3 and IMAP.</li> <li>8. Should support Clean Virtual Private Network (VPN) technology</li> <li>9. Should support 15000+ signature in the Gateway Antivirus (GAV)</li> <li>10. Firewall + IPSEC VPN + SSL VPN</li> <li>11. UTM should have integrated SSL VPN gateway functionality.</li> <li>12. UTM should at least be comprised of following 7 security functionalities 1) UTM + IPSecVpn +SSL VPN 2)Intrusion Prevention system 3)Antivirus 4) Web Content Filtering 5) Application Control 6) Link Load balancing &amp;Router</li> <li>13. The UTM System shall comply with RFC 1918 with support for Static &amp; Dynamic Network Address Translation and Port Address Translation.</li> <li>14. UTM Should not have any user based licensing for UTM and VPN (IPSEC and SSL).</li> <li>15. The UTM should support 802.IQ Trunking and should support minimum 10 Vlans.</li> <li>16. Support for deployment of the UTM in a secure Layer 2 bridging mode, providing rich Layer 2-7 UTM security services for the protected network while remaining "invisible"to devices on each side of it.</li> <li>17. UTM should have access control and deep inspection UTM services for native IPv6 network environments and mixed IPv4 and IPv6 network environments through dual stack support.</li> <li>18. The UTM should support standard routing protocols like RIP, OSPF and BGP in addition to static and policy based routing.</li> <li>19. UTM should support for SSHv2, Telnet, HTTP and HTTPS based management</li> <li>20. UTM should Support for RADIUS, Active Directory &amp;LDAP for the user authentication protocols in addition to local authentication.</li> <li>21. UTM should support Active/Passive High Availability deployment.</li> <li>22. The UTM should have Integrated specialized inspection possible for protocols like HTTP, FTP, DNS, SNMP, ICMP, NFS, H.323, SIP, RTSP and many more.</li> <li>23. UTM should support both SNMPv1, SNMPv2 providing in-depth visibility into the status of appliance.</li> <li>24. UTM Should support both SNMP and email based alerts, UTM should support extensive logging to external logging device or syslog servers and should provide a web</li> </ol> |   |

|  |   |
|--|---|
|  | <p>b ased real time log viewing and filtering capability.</p> <p>25.UTM should support Multiple Link load sharing/balancing</p> <p>26.UTM should support manual content as well as URL filtering support and also support User based UTM policies in addition to IP address based UTM policies</p> <p>27.UTM should identify and control applications regardless of port and protocol for At least 4000 applications.</p> <p>28.UTM should support Traffic shaping and prioritization based on Per IP address</p> <p>29.The product should have IPv6 ready logo that demonstrates readiness for IPv6 Environment</p> <p>30.The proposed system shall comply/support industry standards, supports without Detailed Specification additional external solution, hardware or modules such as IPSEC VPN, , SSL VPN</p> <p>31.The device shall utilize inbuilt hardware/software VPN acceleration for IPSEC (DES,3DES, AES) encryption/decryption and SSL encryption/decryption</p> <p>32.The system shall support IPSEC and PPTP VPN pass through so that computers or subnets on internal network can connect to a VPN gateway on the Internet</p> <p>33.The system shall support Multiple forms of site-to-site VPN configurations Like Route, Policy, Domain etc</p> <p>34.The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode</p> <p>35.The proposed system shall support TWO modes of SSL VPN operation: 1)Web-only mode: for thin remote clients equipped with a web browser only and support web application such as HTTP/HTTPS Proxy, FTP, Telnet and 2) Tunnel mode, for remote computers that run a variety of client and server applications</p> <p>36.The proposed system shall provide certificate-based authentication for administrative</p> <p>37.access to IP Sec &amp;SSL VPN</p> |
| <b>Intrusion Prevention System (IPS)</b>   | UTM should have Integrated IPS Solution   |
|  | Support Behaviors analysis and signature based analysis with online download support of newer signatures for at least 1500 and shall be demonstrated by the firm during inspection and registration.  |
|  | There should be an option to create User-specified signatures.  |
|  | The software on the IPS should support online software reconfiguration to Ensure that changes made to a IPS configuration take place with immediate effect.   |
|  | The IPS should have high availability, so that in case if the primary fails the secondary appliance will become active without any manual intervention  |
|  | 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.   |
|  | IPS solution should be flexible enough to configure, enable/disable signatures and have different actions for the IPS signature at the UTM policy level and not configured at GLOBAL or interface level   |
|  | DOS and DDOS protection should be applied and attacks stopped before UTM policy lookups, AV scan. Option to configure and set DOS threshold values at a IP and Subnet level should be possible  |
|  | 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)   |
| Can export reports to other formats. Should be able to output report data into a variety of different file formats like HTML, PDF and.Doc etc. |   |
| <b>Anti-Virus</b>  | UTM should have integrated gateway level Anti-Virus Solution  |

|                                   |  |
|-----------------------------------|--|
|                                   | <p>Virus gateway should provide real-time detection of viruses and malicious code at the gateway for SMTP, IMAP/ POP3, HTTP, HTTPS and FTP Internet traffic. IM protocols (MSN, Yahoo etc). The solution should detect and block viruses in HTTPS traffic.</p>   |
|                                   | <p>UTM Should support both Proxy based and flow based AV scanning Technology.</p>  |
|                                   | <p>The proposed solution should be licensed per Hardware/Appliance as against per user</p>   |
|                                   | <p>Virus Gateway should have option to configure to respond to virus detection in Several ways .ie. delete the file/quarantine the file and alert e-mail<br/>Frequent updates of virus pattern files should be available from the Web and option for scheduling for automatic update thru a secure communication as well as for manual update should be available.</p> |
|                                   | <p>Should have facility to block files based on file extensions or original file type over HTTP, HTTPS, FTP, SMTP, POP3</p>  |
|                                   | <p>Should have not have any limit of file size for AV Scanning</p>   |
|                                   | <p>The solution should support load balancing for the AV scanning, so that the traffic which needs to be scanned can be load balanced across the boxes in the cluster. Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.</p>                           |
| <b>Anti-Spam</b>                  | <p>The proposed UTM shall have upgradability to provide Anti-Spam capabilities over SMTP, POP3 with External solution, devices or hardware modules.</p>  |
|                                   | <p>Solution should have inspection facility on the header and body of the mail to check for spam URI content and identify whether the mail is a spam mail or not.</p>  |
|                                   | <p>Option should be available to manually configure multiple RBL servers to check for spam mail</p>  |
|                                   | <p>Should have options to configure white list as well black list based on IP address, email address/domain and validate against the same to detect whether a mail is spam mail or not</p>   |
|                                   | <p>Should have provision to define banned key words and check against those key words to identify spam mails.</p>  |
|                                   | <p>Should have configurable spam actions for detected spam mails ie. tag the mail, delete the Spam mail etc.</p>   |
| <b>Web &amp;content Filtering</b> | <p>UTM should have integrated category based URL filtering solution which should be capable of filtering HTTP and HTTPS based URLs</p>   |
|                                   | <p>The proposed solution should be licensed per unit as against per user</p>   |
|                                   | <p>Should be able to block different categories/sites based on users for at least 20 million sites under 50 categories and same shall be demonstrated by the firm during registration and inspection</p>   |
|                                   | <p>Should have configurable parameters to block/allow unrated sites</p>  |
|                                   | <p>Should have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable</p>   |
|                                   | <p>Should have options to customize the block message information send to end users</p>  |
|                                   | <p>Should have facility to configurable policy options to block web sites based on Banned words.</p>   |

|   |  |
|---|--|
|   | Should have configurable policy options to block URLs based on web patterns (e.g. Mail.* to block web mail related sites)  |
|   | Should have configurable policy options to define the URLs what needs to be blocked as well as the exempt list   |
| <b>Application Control</b>  | The proposed system shall have the ability to detect, log and take action against network traffic based on over 1,000 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   |
|   | The proposed system shall have the ability to identify, block or rate limit the following common P2P applications: Gnutella (Napshare, iMesh, Mldonkey, morph, Xolox, BearShare, FOXY), Bittorrent, Kaaza, WinY, edonkey |
|   | The proposed system shall have the ability to manage and control Instant messaging usage by identifying various IM applications such as AIM, MSN, YAHOO, SIMPLE, ICQ   |
|   | Identify IM usernames automatically, thereafter allow administrators to specify access rights accordingly for IM applications like Yahoo, MSN etc  |
|   | Control file transfer and audio call over AIM, ICQ, MSN &Yahoo!  |
|   | The proposed system shall have the ability to manage and control VoIP usage.   |
|   | The unit shall maintain statistics on selected IM and P2P applications, and VoIP Protocols internally.   |
|   | <b>Link and Load Balancing/sharing &amp;Router</b>   |
| The system must be able to support routing protocols including, RIPv1 &v2, OSPF, BGP.                 |  |
| The system shall be able to provide Wan link redundancy using ping probes                             |  |
| UTM should support Multiple links( more than 2) load sharing / balancing with failover cum redundancy |  |



## Annexure – E

| <b>Technical Specification</b>   |                     |                   |                           |
|--|---------------------|-------------------|---------------------------|
| <b>Modular DC 2-Rack Solution with 10 KVA * 2, 2 Ton PAC/Chiller *2 with remote monitoring facilities</b>                |                     |                   |                           |
| <b>General</b>   | <b>Descriptions</b> | <b>Compliance</b> | <b>Remarks/Deviations</b> |
| Usable 'U' Space (Approx)  | 45                  |                   |                           |
| No. of Racks   | 2                   |                   |                           |
| Cooling Redundancy   | Yes                 |                   |                           |
| Cooling Capacity   | 2 x 7 KW            |                   |                           |
| UPS Capacity (UPS will be kept outside of Rack)  | 2 x 10 KVA          |                   |                           |
| UPS Redundancy   | Yes                 |                   |                           |
| Combined Backup Time   | 20 Minutes          |                   |                           |
| Fire Detection   | Yes                 |                   |                           |
| RDU (Rack Data Unit)   | Yes                 |                   |                           |
| Temp. Monitoring   | Yes                 |                   |                           |
| Humidity Monitoring  | Yes                 |                   |                           |
| Door Switch Sensor   | Yes                 |                   |                           |
| Water Leak Sensor  | Yes                 |                   |                           |
| Beacon   | Yes                 |                   |                           |
| Event Alerts   | Yes                 |                   |                           |
| RS 485 Port  | Yes                 |                   |                           |
| Standard Rack PDU (vertical)- with 16 Sockets (12 IEC C13 and 4 IEC C19  | Yes                 |                   |                           |
| SNMP   | Yes                 |                   |                           |
| Email Notification   | Yes                 |                   |                           |
| Blanking Panel 20%   | Yes                 |                   |                           |
| Required Accessories (Keyboard Tray, Component Shelf, Cable Manager, Cable Root, Earthing Copper Strip with insulators ) | Yes                 |                   |                           |