



**Request For Proposal  
For  
Design, Site Preparation,  
Supply, Installation, Commissioning,  
And Maintenance & Operations  
Of The Haryana State Data Centre**

**Volume – II**

RFP no. HARTRON/Proj/State Data Centre-0109/2008-09

Dated: 21.01.2009

**IMPLEMENTING AGENCY**

**Haryana State Electronics Development Corporation Limited**

ISO 9001 Organization

S.C.O. 111-113, Sector 17-B, Chandigarh – 160017 (India)

Ph. 0172-2704922, 2710743, 2706105, 2722961-62, Fax-0172-2705529,

Website: [www.hartron.org](http://www.hartron.org), [www.haryana.gov.in](http://www.haryana.gov.in)

**Table of Contents**

I –	Technical Requirements .....	5
1.	SDC Architecture – IT.....	5
2.	Technical Specifications - IT Components .....	7
2.1.	Core LAN Switch .....	7
2.2.	Application Switches.....	8
2.3.	Internet Router .....	9
2.4.	HIPS (Host Based Intrusion Prevention System).....	11
2.5.	Intrusion Prevention System.....	11
2.6.	External Firewall.....	12
2.7.	Internal Firewall .....	13
2.8.	Database Servers (Intel / AMD64) .....	15
2.9.	Application Server, Web Servers, Enterprise Access Servers, Management Servers, Directory Server, Enterprise Backup Server, Staging Server, Antivirus Server (Blade Server).....	16
2.10.	Work Station ( Desktop) .....	17
3.	Storage and Backup Solution .....	18
3.1.	SAN Switch – Qty02 .....	18
3.2.	SAN .....	18
3.3.	SAN Storage Management Software.....	19
3.4.	Tape Library-Qty01 .....	19
3.5.	Virtual Library System (VLS or VTL) .....	20
3.6.	Backup Software .....	21
3.7.	Server Load Balancer.....	22
4.	Management & Monitoring System (EMS).....	24
4.1.	Design Specifications for EMS.....	24
4.2.	Solution Specifications for EMS.....	26
4.2.1.	Directory Services .....	40
4.2.2.	DNS .....	40
4.2.3.	Anti-Virus .....	41
5.	KVM.....	43
6.	Cabling.....	46
7.	SDC Architecture – Physical Infrastructure .....	50

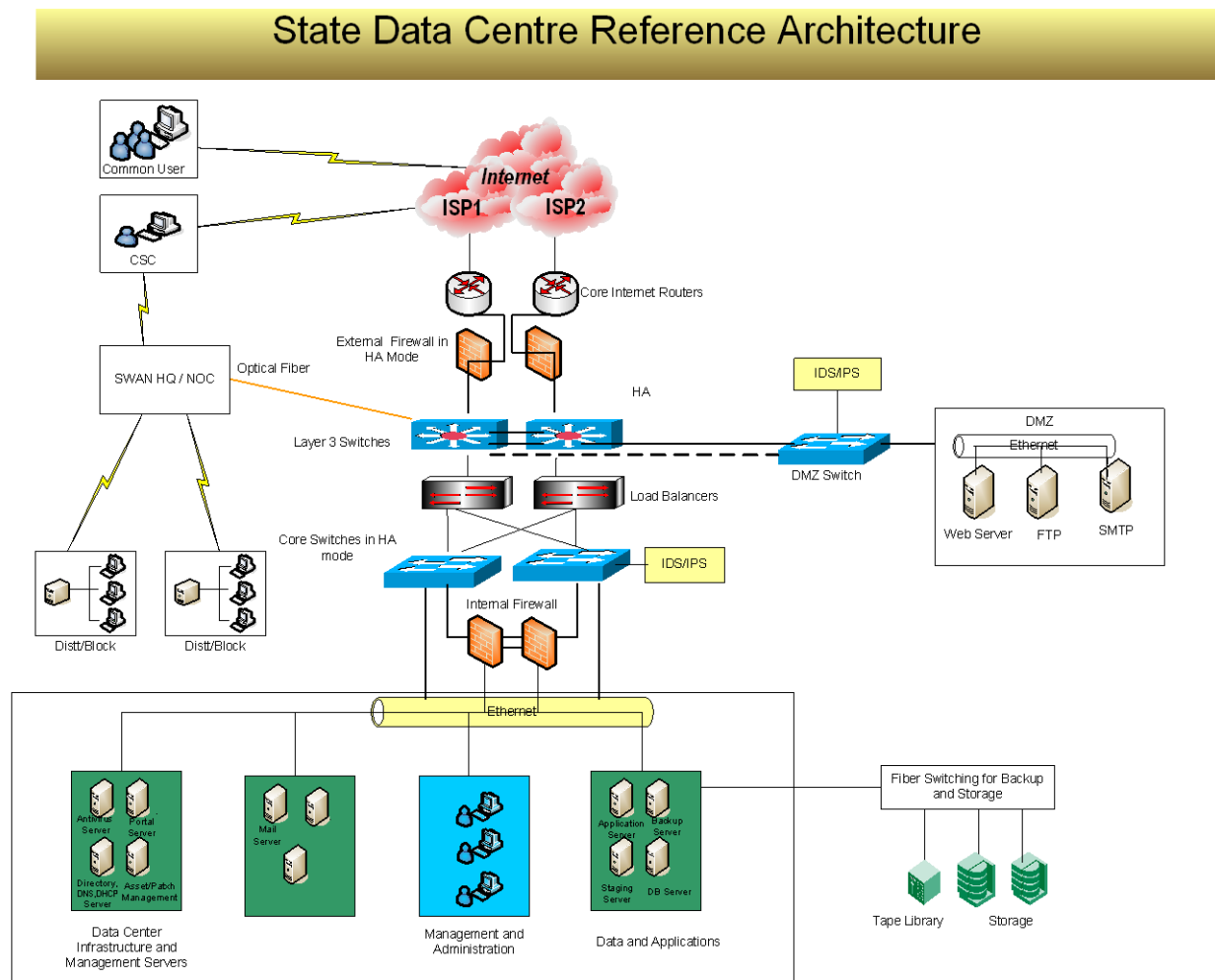
7.1.	Server Farm Area .....	51
7.2.	NOC and Helpdesk Room .....	51
7.3.	Backup & Media Storage Area .....	51
7.4.	UPS & Electrical Room .....	52
7.5.	Alternative Solution .....	52
7.6.	Cost of power and Water during implementation.....	52
8.	Heat Ventilation and Air Conditioning Systems .....	53
8.1.	Air conditioning .....	53
8.2.	Flexibility .....	54
8.3.	Additional Points .....	54
8.4.	Refrigeration controls, condenser and dual blower .....	55
9.	Rodent Repellant .....	57
10.	False Ceiling .....	58
11.	UPS Requirements & Features .....	58
12.	Diesel Generator Set .....	61
13.	Electrical Work for SDC .....	62
13.1.	Electrical panel and Distribution boards .....	62
14.	Technical Specifications – Physical Components.....	64
14.1.	UPS.....	64
14.2.	Diesel Generator Set.....	65
14.3.	Racks: For housing of all the data center component.....	67
14.4.	Jack Panel and Jacks .....	71
15.	Civil & Architectural work.....	71
15.1.	Flooring.....	72
15.2.	Access Flooring : .....	72
15.3.	False Ceiling .....	73
15.4.	Furniture and Fixture .....	74
15.5.	Partitions .....	75
15.6.	Painting.....	76
15.7.	Civil Work.....	76
15.8.	PVC Conduit.....	77
15.9.	Wiring .....	77
15.10.	Lighting Fixtures .....	79

15.11. Earthing .....	79
15.12. Cable Work.....	80
16. Fire Detection and Control Mechanism.....	83
16.1. Fire Suppression System .....	86
16.2. System consideration and requirements .....	90
17. Air conditioning system .....	91
18. High Sensitivity Smoke Detection System .....	97
19. Access Control System .....	97
20. CCTV System.....	100
21. Building Management System (BMS) .....	104
22. Water Leak Detection System .....	105
23. Public Address System.....	105
23.1. Common Alarm System.....	105
24. Fire Proof Enclosures for Media Storage .....	106
25. Electrical Panels .....	109
26. Compliance to Specifications.....	119
27. Glossary of Abbreviations .....	121

# I – Technical Requirements

## 1. SDC Architecture – IT

A typical SDC architecture is being depicted in the schematic below:



### a. Integration of SDC with SWAN

One of the most important aspects which should be taken care while designing the SDC is about seamless integration with SWAN and CSC. The SWAN Network Operating Center( NOC) is situated adjacent to the proposed site of Data center. Presently 1 State Network Center, 22 District Head Quarters, 110 District Network Centers, 120 Blocks are presently connected and working. The SWAN and

Data Center will be directly integrated using optical Fiber. Provisioning of connectivity between the SDC and SWAN shall be the responsibility of SWAN operator.

**b. Internet bandwidth at SDC**

DCO shall be responsible for provisioning of internet bandwidth. The requirement for the same is as under.

Initially the internet bandwidth that will be required for running this centre will be 8 MBPS unshared bandwidth to start off with as all CSC's would be accessing SDC in first phase. In the quarterly review, the DCO will present the bandwidth status and will project the bandwidth requirement if any.

## 2. Technical Specifications - IT Components

### 2.1. Core LAN Switch

- Hardware Architecture (19" Rack mountable)
  - Redundant Supervisor / Switching / Routing engine. All the relevant hardware should be loaded to achieve the required switching and routing performance. Redundancy should be on supervisor on different switching fabric.
  - Internal Redundant Power Supply
  - Power supply 230 Volt 50Hz input
  - Modular Chassis
- Interfaces / Slots
  - Minimum 7 Slots
  - 4 x 48 Ports GE (10/100/1000 MBPS) and upgradeable
  - 1 x 24 Ports Gig Fibre
- Performance
  - High back plane speed 600 GBPS or more
  - Forwarding rate should be atleast 300 MBPS (non-blocking)
- L2 Features
  - IEEE 802.1Q VLAN encapsulation
  - 802.1s
  - 802.1w
  - IGMP snooping v1 and v2, v3
- IP Routing Protocols
  - Static Routing
  - OSPF, OSPF V3
  - RIP, RIPng
  - HSRP /VRRP
  - IPv4 / IPv6 support
- Security
  - Standard and extended ACL's on all ports
  - AAA and RADIUS authentication
- Manageability & Up gradation

- Console port for administration & management
- Support SNMP v1, v2,v3
- Support management using CLI, GUI using Web interface
- Support FTP/TFTP for upgrading the operating System
- Standards
  - IEEE 802.1x support
  - IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports
  - IEEE 802.1D Spanning-Tree Protocol
  - IEEE 802.1p class-of-service (CoS) prioritization
  - IEEE 802.1Q VLAN
  - IEEE 802.3 10BASE-T specification
  - IEEE 802.3u 100BASE-TX specification

## 2.2. Application Switches

Application switches shall be implemented in the DMZ and shall be connected to the core LAN switch and the router.

- **Rack Mountable:** Mountable in standard 42U rack.
- 48 ports, 10/ 100/1000 Base auto-sensing with 4 Nos. GBIC/SFP Slots
- Atleast one console port for CLI based configuration
- 30 GBPS switching fabric
- 35 MBPS forwarding rate
- IEEE 802.3ad support required
- Link Aggregation Control Protocol (LACP) to aggregate 4x1GBPS i.e. 4GBPS uplink to the Core LAN Switch.
- Load Balancing and Failover support should be built-in
- **Management:**
  - SSH v2,SNMP v1/v2c/v3,IGMPv3, RMON I, VLANs, GUI, Web based interface,
  - Compatibility with network mgmt with auto discovery & management.
  - Manageability on per port basis.
- **Security:**
  - 802.1x support,
  - RADIUS support

- MAC address based port level filtering support
- **Quality of Service:** The switches should support the aggregate QoS model by enabling classification, policing/metering & marking functions on a per-port basis at ingress and queuing/scheduling function at egress
  - The switches should support QoS classification of incoming packets for QoS flows based on Layer 2, Layer 3, and Layer 4 fields.
  - The switches should support identification of traffic based on Layer 3 ToS field – DSCP values.
- Support for rate limiting with granularity of traffic flows.
- TFTP & NTP support,
- Compliant to Standards such as IEEE 802.1x, 802.1w, 802.1s, 802.3x, 802.1D, 802.1p, 802.1Q, 802.3ad, 802.3u, 802.3ab, 802.3z

### 2.3. Internet Router

- Hardware Architecture (19" Rack mountable)
  - Should support IP, MPLS etc
  - Power supply supporting hot swappable functionality.
  - On-line insertion and removal for cards
  - Modular Chassis
  - Power supply for 230 V AC 50 Hz with Redundant power supply
- Interface / Slots
  - Ethernet Port 10/100 MBPS
  - Should support variety of interfaces like ChE1/E1/ISDN PRI/ ChE3
  - Console port
- Security
  - GRE and IP Sec 3DES/AES VPN for configuration of VPN tunnels.
  - NAT, PAT
  - Access control - Multilevel
  - Support ACL's to provide supervision and control.
  - Multiple Privilege Levels for managing & monitoring
  - Support for Remote Authentication User Service (RADIUS) and AAA
- Routing Protocols
  - Static Routes

- RIPv1, RIPv2
- OSPFv2 and v3.
- BGP4
- Route redistribution between any of the above protocols
- It should support Load Balancing on equal and un-equal cost paths
- Protocols
  - PPP, Multi-link PPP
  - HDLC
  - IPv4, IPv6
  - MPLS L2 & L3
  - VRRP / HSRP
- Congestion
  - Random Early Detection
  - Weighted Fair Queuing
  - Selective Packet Discard
- IP Multicasting
  - IGMPv1,v2& v3, PIM-SM, PIM-DM or MOSPF
- Management
  - Accessibility using Telnet, SSH, Console access.
  - Software upgrades using FTP, TFTP, etc.
  - SNMP Support for v1, v2
  - Using CLI, GUI based software utility and using web interfaces
  - Support for Syslog
- Debug & Diagnostics
  - Display of input and output error status on all interfaces
  - Display of Dynamic ARP table
  - Display of physical layer line status signals like DCD, DSR, DTR, RTS, CTS on all interfaces
  - Display of Routing table
  - Trace-route, PING, extended PING

## 2.4. HIPS (Host Based Intrusion Prevention System)

- HIPS should perform log analysis, integrity checking, root kit detection, time-based alerting and active response. It should help to detect attacks, software misuse, policy violations and other forms of inappropriate activities.
- HIPS should be able to monitor multiple systems, with one system being the HIPS server and the others the HIPS agents that report back to the server.
- Minimum Features of Host-based intrusion Prevention:
  - Time to Time Signature updates
  - Monitoring and prevention from Intrusion attack
  - Monitors specific system
  - Detects attacks that network-based systems miss
  - Well-suited for encrypted and switched environments
  - Near-real-time detection and response

## 2.5. Intrusion Prevention System

- Features
  - Layer 7 Throughput of 4 Gigabit or more
  - Minimum 4 Numbers of Gigabit segments support. Option for future expansion to add 4 more Gigabit segments should be provided.
  - Should support monitoring of 2 inline segment from day one and should be upgradable to 4 inline segment
  - Should support fail-open to four Gigabit segments in case of HW/SW failure
  - Should protect against DoS/ DDoS / SYN-flood/ TCP-flood /UDP-flood
  - Must have “Zero-day” protection against DoS/DDoS and worm attacks based on traffic behavior. Also it should mitigate Zero day http floods and brute force attack & vulnerability scanning attempts based on traffic behavior analysis
  - Capable of applying the security policies based on VLAN ID, Source/Destination subnets
  - Should protect against SSL based attacks by integrating with external high capacity SSL accelerators.
  - Should support peer to peer traffic detection & blocking and rate shaping for P2P traffic.
  - Should support bandwidth management and QoS provisioning
  - Should protect against XML based crafted messages
- Action on detection
  - Block attacks in real time, Drop Attack Packets, Packet Logging

- Reset Connections, Action per Attack
  - Support for detailed intrusion alarms
- State Operation
  - TCP Reassembly
  - IP Defragment
  - Bi-directional Inspection
  - Forensic Data Collection
  - Access Lists
- Signature Detection
  - Vendors Signature Database of minimum 1500 signatures
  - Device should have capability to add User Defined Signatures
  - Should support Automatic signature synchronization from OEM database server.
- Extensive protocol monitoring: should support monitoring of protocols such as TCP/IP, ICMP, FTP, UDP, SMTP, HTTP, SNMP, DNS, RPC, NetBios, Telnet etc
- Should also have the ability to monitor 802.1 (trunked) traffic.
- Certification ( Should have atleast one)
  - ICSA/ Common Criteria (EAL)/ NSS/ FIPS
- Alerting SNMP, SMTP support
  - Log File, Syslog support
- Management
  - Console, SSH, Telnet, HTTPS, HTTP, SNMP v1, v2

## 2.6. External Firewall

- Physical attributes
  - Should be mountable on 19" Rack
  - Modular Chassis
- Interfaces
  - Should have atleast 4x GE upgradeable to 8x GE,
  - Console Port, 1 number
- Performance and Availability
  - Redundant Architecture
  - Firewall Throughput: minimum 4GBPS

- Encrypted throughput( 3 DES/AES): minimum of 1.0 GBPS
- Concurrent connections: up to 60,000 numbers
- Simultaneous VPN tunnels: up to 10,000 numbers
- Memory
  - Minimum RAM 1024 MB, Upgradeable to 2048 MB RAM
  - Flash 256 MB Upgradeable to Flash 512 MB
  - Encrypted throughput: minimum 800 MBPS
  - Concurrent connections: up to 2,000,000
  - Simultaneous VPN tunnels: 2000
  - Clear text throughput: Up to 07 GBPS
- Protocols
  - TCP/IP, PPTP
  - RTP
  - IPSec, DES/3DES/AES
  - PPPoE
  - FTP, HTTP, HTTPS
  - SNMP, SMTP
  - DHCP, DNS
  - support for IPv6
- Other support
  - 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Layer 2 Firewall, Virtual Firewall, Radius/TACACS
- Management
  - Console, Telnet, SSHv2, Secured GUI based configuration.
  - SNMPv1, SNMPv2

## 2.7. Internal Firewall

- Hardware Architecture
  - Modular chassis
  - 19" rack mountable
  - Shall Support At least 5 Security Zones physically with 1 GBPS ports isolated from each other

- Statefull Inspection
  
- Performance
  - The firewall throughput performance should be at least 5GBPS or more.
  - Should support 3DES/AES VPN Throughput of atleast 1 GBPS
  - The firewall should provide at least 50,0000 or more concurrent connections
  - Should provide at least 50,000 connections per second or more.
  - Should support 802.1Q trunking and at least 50 VLANs.
  - Should have AAA through RADIUS or TACACS (RFC 1492) protocol and should support with the AAA server asked for the network.
  - Should have Application inspection for standard applications like DNS, FTP, HTTP, ICMP, MGCP, NetBIOS Name Service, SMTP, TFTP etc.
  - Should support inbuilt support for IPSEC VPNs with DES/ 3DES and AES support.
  - Firewall should support MD-5 and SHA-1 authentication
  
- Firewalling at layer 2 and layer 3 of the OSI layer.
  - Static route, RIPv2, and OSPF
  - NAT and Port Address Translation feature
  - Optional support to perform intelligent packet filtering, URL filtering.
  - Should support IPv4 and IPv6.
  - Optional support to be able to detect, respond to and report any unauthorized activity.
  
- Firewall features shall include:
  - Application/Protocol Inspection Engines:
  - L2 transparent firewalling
  - Advanced HTTP Inspection Engine
  - Time-based ACLs
  
- VPN feature shall support:
  - Support for n-tiered X.509 certificate chaining
  - Manual X.509 certificate enrollment (PKCS 10/7 support)
  
- Authentication, Authorization and Accounting (AAA) Features:

- Support multiple RADIUS accounting servers
- Accounting for management traffic - generates AAA accounting records for management connections to the device.
- Native Window NT/Active Directory user authentication support (VPN only)
- Native SDI/RSA SecurID user authentication support (VPN only)
  
- High Availability – State full failover
- Management
  - Embedded web based configuration / management support.
  - Should have Management access through console, SSH and GUI for managing the firewall.
  - Should have the capability of restricting the access through the Console and out-of-band management interface to protect the devices from local threats.

## **2.8. Database Servers (Intel / AMD64)**

- Minimum 2x Quad core processor with 2.1GHz or above with 1066Mhz FSB expandable to four physical processor with 2x2MB I2 cache per processor
- Minimum Memory: 8 GB, Scalability to 128 GB
- HDD 4x146GB 2.5" 10K RPM HDD or More
- Redundant Power Supply
- Atleast 2 x 10/100/1000 MBPS Ethernet Ports
- 2 x 4 GBPS Fiber Channel ports. This is required only for database servers.
- RAID Controller with RAID 0/1/5 with 256 MB cache and does not occupy any PCI slot
- Optical / diskette: 8X / 24X slim-line DVD ROM drive
- Remote Management hardware to monitor server remotely even when server power is off.
- Management Feature to identify failed components even when server is switched off.
- Server components should be UL, FCC, IEC,EN and ROHS complied.
- Rack Mountable
- It should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet.
- Should be able to manage systems through a web-browser

## 2.9. Application Server, Web Servers, Enterprise Access Servers, Management Servers, Directory Server, Enterprise Backup Server, Staging Server, Antivirus Server (Blade Server)

- Single blade chassis should accommodate minimum 6 (Quad-Processor)/8 (Dual Processor) and Scalable to minimum 10 or higher hot pluggable blades
- 6U to 12U Rack-mountable
- Dual Back-plane providing 2 separate connections to each Blade Server or single Passive Backplane.
- Should accommodate Intel, AMD, RISC/ EPIC Processor based Blade Servers for future applications
- Should be certified for installing all industry standard flavors of Windows, LINUX/LINUX/UNIX and LINUX/UNIX Operating Environments
- Single console for all blades in the enclosure or KVM Module/ feature or access through centralized console.
- DVD ROM can be internal or external or through centralized console, which can be shared by all the blades allowing remote installation of S/W and OS.
- Two 10/100/1000 Ports per blade.
- Two hot-plug, redundant 4 GBPS Fiber Channel adapters per blade. It should connect to the external Fibre Channel switch, and ultimately to the storage device.
- **Power Supplies:**
  - Chassis to be fully populated with hot Swappable redundant power supplies
  - Power supplies should have N+N or N+1 redundancy. All Power supply should be populated.
- Hot Swappable and redundant Cooling Unit
- All Cooling Modules/Fans should be populated. LED indicators Alerts on Hard disk drives, processors, blowers/Fans, memory or provision to monitor the same.
- **Management:**
  - Systems management and deployment tools to aid in Blade Server configuration and OS deployment,
  - Remote management capabilities through internet
- Built-in KVM switch (Chassis should have provision of accommodating Optional redundant KVM switch) or KVM functionality provisioned through chassis.
- Dedicated management network port should have separate path for management

- Support heterogeneous environment: Xeon and RISC/EPIC CPU blades must be in same chassis with scope to run Win2008 Server, Red Hat LINUX/LINUX/UNIX, Suse LINUX/LINUX/UNIX, 64 Bit LINUX/UNIX.
- **Blade Specifications:**
  - Blade can be half/full height
  - 2 Quad core 2.3 Ghz/ 2 Dual core @ 3GHz with 4 MB shared L2 cache, 1333 MHz FSB
  - 4 GB DDR2 RAM with 2 No's free slots for future expandable capability.
  - Memory upgradeable to atleast 16 GB or higher per blade.
  - The Blade should have redundant 4 GBPS Fiber Channel HBA
  - 2 X (1000BASE-T) Tx Gigabit LAN ports support on blade server
  - 2 X 146GB HDD or more hot plug system disk with mirroring using integrated RAID 0,1 on internal disks
  - VGA/Graphics port
  - Should support heterogeneous OS platforms

## 2.10. Work Station ( Desktop)

- The system software for RDBMS must provide all the administration tools, notification server:
- CPU should have Intel Pentium Dual Core E2140 (1.6 GHz, 1 MB L2 cache, 800 MHz FSB) / AMD\* Athlon\* 64 X2 4000+ (2.1 GHz, 2\*512 KB L2 cache, 2000 MHz FSB, AM2 socket)
- Motherboard should have For Intel (Intel G31 chipset or better ), For AMD (AMD 690 series with Radeon 1200 Graphics or NVIDIA GeForce 6150 chipset or better)
- Bus Architecture Integrated onboard graphics, Two PCI, One PCI Express 1/4, One PCI Express 16 slots ,Integrated Audio
- Memory should have 1 GB DDR2 SDRAM @ 667 MHz. 1 DIMM slot should be free.
- Hard disk should have 160 GB SATAII hard disk with 7200 rpm & Pre Failure alert.
- Keyboard should be USB or Ps/2 104 Keys keyboard.
- Mouse should be USB or PS/2 Two button scroll optical mouse with pad.
- Ports are 1 Serial, 1 Parallel, 4 USB 2.0 (min. 2 at front), VGA, Microphone, Headphone. Networking features like 10/100/1000 MBPS Network card.
- O.S. should have Pre loaded Windows XP Professional licensed software with latest updates and Restore/ Recovery CD/ Self Mechanism
- Certifications For PC: Windows XP certification
- For Monitor: MPR II/TCO 03 certification
- Antivirus should have Pre loaded Latest Trend Micro Anti virus software with license and media with one year updates

- Dust Cover for CPU, Monitor, Keyboard, Mouse

## **3. Storage and Backup Solution**

### **3.1. SAN Switch – Qty02**

- Minimum 16 Active ports (each with minimum port speed 4Gb) within same switch upgradeable to 32 ports with minimum 2 no of additional 10GBPS FC ports.
- Should support FCIP protocol
- All cable and accessories for connecting Servers /Devices to SAN
- Should have capability of port trunking.
- Should have dual Fans and Hot plug power supplies
- Should have GUI based management software for administration and configuration
- Should support zoning configuration, virtual SAN/ Virtual Fabric
- Should support fabric routing to enable cross fabric connectivity
- All other necessary fiber cables and racking accessory should be supplied
- Should have inbuilt diagnostic features like power on self test, FC trace route, FC ping
- Should support RADIUS authentication or SSH

### **3.2. SAN**

- Dual active-active storage Controllers and SAN raid array in an end-to-end 8 GBPS architecture.
- The storage array should support industry-leading Operating System platforms and clustering including: Windows Server 2008 (enterprise Edition), sun Solaris, HP-UX, IBM-AIX, LINUX/UNIX etc.
- The storage array shall be configured with atleast 4 GB cache of total cache mirrored across with dedicated interface / paths communication between two storage controllers and should be scalable to 8GB.
- All the necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, virtualization, snapshots (including snap clones and snap mirrors) for entire capacity etc.
- Redundant and hot swappable power supplies, batteries and cooling fans and data path and storage controller.
- Load balancing must be controlled by system management software tools
- The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for upto 72 hours or more.

- The offered system should be pre-configured with at least 10 TB of useable Storage Capacity out of which 5TB useable shall be configured using Fiber Channel Hard disks of at-least 300 GB or higher 15 K PRM drives in RAID 5 and 5TB useable capacity shall be configured using 750GB or higher SATA/FATA Drives. The Storage should have at least 32GBPS port bandwidth for the connectivity to servers and at least 16GBPS port bandwidth (aggregated) for disk connectivity.
- Storage should support hardware based RAID with RAID level 0, 1, 5
- Appropriate hard disks of different capacities should be included in the offer and priced separately (300 GB 15 KRPM, 1 TB SATA/FATA etc).
- Storage must be offered with Global Hot Spare Disk drive at least 1 Disk Drive per 30 Disk configured rounded off to next number for both FC and SATA/FATA Drives.
- The storage array must have capability to do array/Controller based remote replication.
- The system array should support synchronous and asynchronous replication.

### **3.3. SAN Storage Management Software**

- Should support storage virtualization, i.e. Easy logical drive expansion
- Should support hot-swappable physical drive raid array expansion with the addition of extra hard disks
- Should support expansion with drives of lower performance like SATA / FATA drives 7.2K RPM.
- Should be able to allocate logical spaces to multiple operating Systems in the same storage facility
- Should be able to support clustered and individual servers at the same time
- Should be able to take "snapshots" of the stored data to another logical drive for backup purposes.
- Should be able to take "snapshots"/Mirror Clones of the stored data to another internal or possibly to another external logical volume.
- Vendor should also offer storage performance monitoring and management software
- The vendor must provide the functionality of proactive monitoring of Disk drive and Storage system for all possible hard or soft disk failure

### **3.4. Tape Library-Qty01**

- Should support LTO-4 or latest technology based library with at least 4 LTO-4 tape drives with more than 50 Ultrium cartridge slot attachable to SAN with FC network, rack mountable.
- Cartridges should have physical capacity up to 800GB per cartridge compressed; 400GB native

### 3.5. Virtual Library System (VLS or VTL)

- Back up would be done in such a way that daily incremental data and on weekend's complete backup will be taken. Also the DCO will adhere to the backup policy as defined by the state, from time to time.
- Virtual Library shall be Modular design to allow configuration, and add capacity to increase performance.
- Virtual Library shall be offered with Minimum of 5TB of useable space scalable to atleast 30TB useable.
- Virtual Library shall have the ability to configure/emulate at-least 16 tape Libraries, 100 or more tape drives and atleast & at-least 512 Cartridge slots in the single appliance.
- Virtual library Solution shall have capability to deliver selective restore from disk Library itself.
- Solution shall integrate and utilize customer's current tape backup infrastructure in the following aspects.
  - Compatibility with the existing backup server/media servers at customer end
  - Compatibility with the existing tape library and tape drive
  - Compatibility with the existing backup software
  - Compatibility with the existing san switch hardware.
- Compatibility with all the leading backup software products and customer backup software specifically.
- Ability to flexibly emulate popular tape drive/tape formats LTO-Gen2, LTO-Gen3, LTO-Gen4, DLT8000, SDLT etc.
- Offered Virtual Library shall have Minimum of 4 x Fibre Channel connections to SAN switches.
- Fault tolerance in the offered Virtual Library shall be achieved by active disk redundancy technology like RAID.
- Virtual Library shall offer Data compression feature with out performance degradation feature without using from back up software, replication support. The bidder shall provide the relevant documents for the same.
- Virtual Library Solution shall allow the backup application's Manager (server that runs the backup application) to handle the movement of data from disk to tape.
- The Virtual Library shall have the ability to add and upgrade disk.
- Management console/interface of Virtual tape library shall provide the following functionality:
  - Add or delete virtual libraries
  - Add or delete virtual tape drives

- Add or delete virtual tape cartridges
- Add new disk storage
- Configure network parameters

### **3.6. Backup Software**

- The proposed Backup Solution should be available on various OS platforms such as Windows and LINUX/UNIX platforms and be capable of supporting SAN based backup / restore from various platforms including LINUX/UNIX and Windows.
- Proposed backup solution shall be offered with Cluster license of server.
- Proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration.
- The proposed backup solution should allow creating tape clone facility after the backup process.
- The proposed Backup Solution has in-built frequency and calendar based scheduling system and supports Clustering the Backup Server and Media Server on Windows and LINUX/UNIX.
- The proposed backup solution supports the capability to write multiple data streams to a Target device which can be a Disk or Tape devices in parallel from multiple clients to leverage the overall throughput of the available devices.
- 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 client/servers
- The proposed solution should be capable of taking back up of SAN environment and well as LAN environment.
- The 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 offered with unlimited client and media (Both Cluster and stand alone) or atleast 100 Client and Media License (Both Cluster and stand alone) for SAN based backup and LAN based backup.
- The proposed solution also supports advanced Disk staging
- The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media.
- Backup Software is able to rebuild the Backup Database/Catalog from tapes in the event of catalog loss/corruption.
- The proposed Backup Software shall offer OPEN File Support for Windows based servers.

- The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, PostgreSQL, DB2, Sybase etc on various OS
- The Proposed backup solution shall provide granularity of single file restore.
- The Proposed backup solution shall be designed in such a fashion so that every client/server in a SAN can share the robotic tape library.
- Backup Solution shall be able to copy data across firewall.
- Backup solution should provide command line utilities an alternative method of accessing the operations available from the GUI Manager.
- Backup solution should also provide report writer that allows designing of report templates which can be used to generate meaningful reports in CSV / HTML / XML / Text format / PDF.

### 3.7. Server Load Balancer

- 10/100/1000 MBPS Ethernet Ports 4 ports
- Throughput support up-to 2 GBPS
- Memory 1 -2 GB
- Server Load Balancing Mechanism
  - Cyclic, Hash, Least numbers of users
  - Weighted Cyclic, Least Amount of Traffic
  - Private/Customized Algorithm, Response Time
- Redundancy Features
  - 1 + 1 Active hardware Redundancy
  - Provision for SLB to work in Active-Active mode
  - VRRP/HSRP Support
  - Segmentation/Virtualization support along with resource allocation per segment, dedicated access control for each segment, CPU, throughput & Access Control per Virtual partition
- Server Load Balancing Features
  - Server and Client process coexist
  - UDP Stateless
  - Service Failover
  - Backup/Overflow
  - Direct Server Return
  - Client NAT

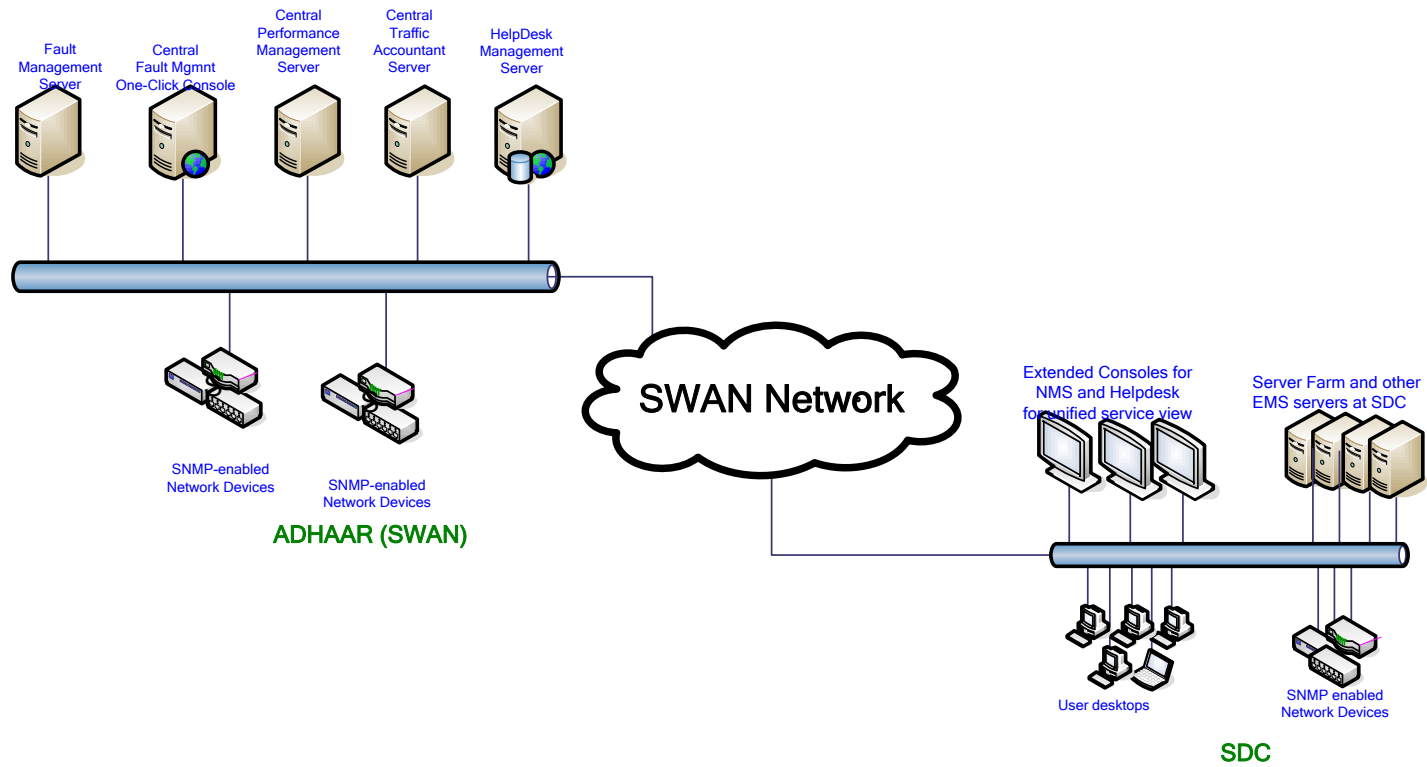
- Port Multiplexing-Virtual Ports to Real Ports Mapping
- DNS Load Balancing
- Next hop router per VIP
- Should support static and dynamic Caching
- Should support TCP offloading
- Load Balancing Applications
  - Application/ Web Server, MMS, RTSP, Streaming Media
  - DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH,
  - LDAP, RADIUS
- Content Intelligent SLB
- HTTP Header Super Farm
- URL-Based SLB
- Compression
  - It should support HTTP based compression
  - Compression Throughput atleast 500 MBPS
- SLB should support below Management options
  - Web Based Management
  - Secure Web Based Management
  - SSH
  - TELNET
  - SNMP v1,2, 3 Based GUI
  - Command Lin

## 4. Management & Monitoring System (EMS)

- The proposed solution should manage service availability of various citizen-centric services hosted in SDC by identifying critical services.
- The proposed solution should provide comprehensive and end-to-end management of all the components for each service including Network, Systems, Databases and Application infrastructure.
- The management system needs to aggregate events and performance information from the domain managers and tie them to service definitions. This capability is critical for the SDC to have a complete view of the performance and availability of various application services being managed.
- The proposed EMS tools should automatically document problems and interruptions for SDC services and integrate with the service level management system for reporting on service level agreements (SLAs).

### 4.1. Design Specifications for EMS

- Monitoring fault and performance of the SDC network components as well as a helpdesk solution for the Data Center is a key requirement for the State. HARTRON has already procured and implemented the following management tools from CA to manage their SWAN:
  - CA SPECTRUM Suite of products for Network fault Management
  - CA eHealth Suite of products for Network Performance Management
  - Unicenter ServiceDesk Suite of products for Helpdesk Management and
  - CA Secure Content Manager Suite for protecting content at the gateway
- The Bidder can quote any tool of his choice, though presently CA is being used. Integration with the existing tool will be the responsibility of the bidder. .
- The suggested deployment architecture for the NMS and Helpdesk Solutions is shown below:



## 4.2. Solution Specifications for EMS

The basic components for this management solution will be as follows:

- **Performance Management** – Provide performance management across key parts of the infrastructure. The solution should integrate network, system and database performance information. It should allow identifying trends in performance in order to avert possible service problems. The proposed performance management system shall **integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network and system components**. The current performance state of the entire network and system infrastructure in the SDC shall be visible in an integrated console.
  - The proposed Network Performance Management System must provide the following features:
    - The extended Network Performance Management consoles must provide a consistent report generation interface from a single central console at SDC.
    - Central console will also provide all required network performance reports (threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure managed by SWAN and SDC..
    - The proposed system shall collect, analyze and summarize management data from LAN/WAN, MIB-II interfaces and various servers for performance management.
    - The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources
    - The proposed system shall provide Performance of Network devices like CPU, memory & buffers etc, LAN and WAN interfaces and network segments.
    - It shall provide comprehensive health reporting to identify infrastructure in need of upgrades and immediate attention. Capacity planning reports shall identify network traffic patterns and areas of high resource utilization, enabling to make informed decisions about where to upgrade capacity and where to downgrade or eliminate capacity. It should also support Trend analysis & Forecasting reporting to enable understanding the effect of growth on available network resources..
    - The proposed system shall provide easy to read representations of health, utilization and availability.
    - It shall provide Real time network monitoring and Measurement offend-to-end Network/ system performance & availability to define service levels and further improve upon them.

- Detailed analysis of performance metrics and response time for the network shall be made available.
- System shall identify how device resources are affecting network performance, document current network performance for internal use and service level agreements (SLA).
- The proposed solution should provide the following performance reports.
  - Executive Summary report that gives an over all view of a group of elements, showing volume and other important metrics for the technology being viewed.
  - Capacity Planning report which provides a view of under-and-over-utilized elements.
  - Service Level report that shows the elements with the worst availability and worst response time-the two leading metrics used to monitor SLAs.
- The proposed system must have a built-in report authoring tool which will enable complete customization flexibility of performance reports.
- The tool should provide performance information from Single Console. It should be possible to drill-down into the performance view to execute context specific reports.
- The proposed system should provide the following reports for troubleshooting, diagnosis, analysis and resolution purposes:
  - Trend Reports
  - Status at a Single View Reports
  - Utilization reports with Top N
  - Capacity prediction reports with What-If analysis

The proposed **Server Performance Management System** must provide the following features:

- The proposed server performance management system shall integrate network performance management systems and provide the unified performance state view in a single console. The current performance state of the entire network and server infrastructure in the SDC shall be visible in an integrated console.
- The proposed tool must provide server agents to ensure availability and performance for target server nodes and deliver scalable, real-time management of critical systems at SDC.
- The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.
- It should be possible to configure the operating system monitoring agents to monitor systems based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.

- The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms including Windows, LINUX/UNIX, and LINUX/LINUX/UNIX.
- It should also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.
- The proposed tool must provide provision for performance scoping and trending to provide real-time as well as historical reporting, where specified.
- The proposed tool should be able to gather information about resources over a period of time and provide historical performance and usage information through graphical reports, which will quickly show performance trends.
- The proposed solution should support management following parameters:
  - **Processors:** Each processor in the system should be monitored for CPU utilization. It should compare Current utilization against user specified warning and critical thresholds.
  - **File Systems:** Each file system should be monitored for the amount of file system space used, which should be compared to user-defined warning and critical thresholds.
  - **Log Files:** Logs should be monitored to detect faults in the operating system, the communication subsystem, and in applications. System agents should also analyze log files residing on the host for specified string patterns.
  - **System Processes:** System agents should provide real-time collection of data from all system processes. Using this it should help identify whether or not an important process has stopped unexpectedly. It should provide an ability to automatically restart Critical processes.
  - **Memory:** System agents should monitor memory utilization and available swap space and should raise an alarm in event of threshold violation.
- The proposed solution should provide automated management to detect, isolate, and resolve problems autonomously
- The proposed solution should provide self-monitoring wherein it will track critical status such as
  - CPU utilization
  - Memory capacity
  - File system space and other important data.
- The proposed tool should detect threshold violations in real-time, send alerts/trapsto the existing network management system at SDC and automatically fix problems according to pre-specified instructions.

- The proposed tool should provide Process and NT Service Monitoring wherein if critical application processes or services in SDC fail, administrators are immediately alerted and processes and services are automatically re-started
- The proposed solution should provide quick at-a-glance reports on systems and applications, disk and file system statistics, hardware/software inventories and more. The tool should be able to identify CPU hogs, and detect memory-leaking processes and I/O bottlenecks before they bring down the server.
- The proposed tool should be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool should notify administrators and enable to take action like sending an email.

The proposed **Database Management System** must provide the following features:

- The proposed database performance management system shall integrate network and server performance management systems and provide the unified performance state view in a single console. The current performance state of the entire network and systems infrastructure in the SDC shall be visible in an integrated console.
- It should be able to automate monitoring, data collection and analysis of performance from single point.
- It should also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.
- Database performance management solution for Distributed RDBMS must include hundreds of predefined scans for monitoring various database, operating system and network resources. This should minimize the need to write and maintain custom scripts. If a special monitoring situation exists, you can modify an existing script to meet your requirements.
- With respect to user-defined parameters, the tool should report conditions that exceed thresholds and automatically takes corrective actions.
- The event management system must send alerts for an array of server conditions, including inadequate free space, runaway processes, high CPU utilization and inadequate swap space.
- The tool should have the ability to create real-time or historical custom graphs and stacks for comparison, correlation and trending across any collected database or database server
- The database performance management solution must support historical archive store for performance information in a compressed time-series form. DBAs should be able to drill down through layers of data to discover the cause of a condition occurring with the databases, operating system or network. These historical reports must also be usable to perform trend analysis and capacity planning.
- The database performance management solution must be able to trace, analyze and tune resource-consuming SQL statements.

- The database performance management solution must have a console to enable users to monitor, analyze and take corrective action from a centralized point. It should also include a platform-independent, browser-based console to monitor performance from remote locations.

The proposed **Service Level Management System** must provide the following features:

- The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, business services shall include E-mail, Internet Access, Intranet and other business services hosted.
- The Users definition facility must support defining person(s) or organization(s) that uses the business Services or is a party to a service level agreement contract with a service provider or both. The facility must enable the association of Users with Services and SLAs.
- The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service Guarantees that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on). Guarantees supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
- Root cause analysis of infrastructure alarms must be applied to the managed Business Services in determining service outages.
- SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
- The system must provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA must be available.
- The system must provide the capability of Advanced Correlation for determining Service health, performing root cause analysis, and fault isolation. This must include applying complex Boolean logic on multiple attributes and infrastructure alarms.
- The system must provide a real time business services Dashboard that will allow the viewing of the current health of required services inclusive of real-time graphical reports.
- The system must provide a historical reporting facility that will allow for the generation of on-demand and scheduled reports of Business Service related metrics with capabilities for customization of the report presentation.

The proposed solution must provide a centralized **Job Management System** to support job scheduling in all common operating system platforms. The proposed solution should be able to support multiple network protocols and be able to combine disparate jobs and processes into a cohesive workflow. The solution should be able to manage and schedule, visualize and optimize

the job flows in real time end-to-end, from a secure, single point of control. The proposed system must comply with the following specifications:

- The proposed Job management solution should support heterogeneous LINUX/UNIX and Windows environments with complete scheduling interoperability
- The proposed solution must adhere to Manager-Agent architecture where agents are only necessary on machines where batch jobs run, managed centrally via a manager
- The proposed solution should not require any persistent connections between manager and agent to minimize resources
- The proposed solution should run on non-proprietary data storage, which supports popularly used RDBMS such as Oracle, Sybase, MS SQL, SQL, DB2 etc.
- The proposed solution should have a Graphical User Interface (GUI) and command line interface for controlling and monitoring of jobs, and creation of jobs.
- The proposed solution should provide a Web-interface for monitor and administration of jobs.
- The proposed solution must support custom calendars and these should be easily defined using a GUI or WEB interface
- The proposed solution should provide graphical representation of job dependencies/job flows that are scheduled to run
- The proposed solution should provide functionality to create complex branching logic based on job dependency.
- The proposed solution should provide the ability to define file watcher jobs to check arrival of a file in a specified folder.
- The proposed solution should support command line interface with support for Job Definition Language
- The proposed solution must ensure that all job dependencies are met before a job is allowed to execute
- The proposed solution should provide functionality to trigger jobs based on success/failure as well as exit codes of other jobs.
- The proposed solution system must have the capabilities to manage the operations of batch jobs. The batch jobs shall include, but not limited to:
  - Ad hoc/routine scheduled jobs
  - Ad hoc/routine scheduled housekeeping jobs
  - Ad hoc/routine scheduled jobs for report generation
- The proposed solution must generate alarms whenever exceptional condition arises such as job failure or processing problems.
- The proposed solution should have functionality to prioritize jobs in terms of importance of job run.

- The proposed solution should support Manual/Automatic restart of failure jobs
- The proposed solution should provide detailed record of processing on starting time, time used for running the job and time of completion
- The proposed solution must integrate out-of-the-box with Enterprise Management solutions for centralized event notification and programmable actions.
- The proposed solution should provide Real-time inspection of job status which must be viewable using command line reports or the Operator Console
- The proposed solution must list all the job dependencies, and display the current state of a job, regardless of the network machine on which it is being run.

**Application Performance Management** – enabling to identify, prioritize and resolve defective transactions — often before they impact users — through real-time visibility into transactions. The proposed **Application Performance Management System** must provide the following features:

- The proposed solution should proactively monitor all user transactions for any web-application hosted in a J2EE-compliant application server; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes
- The proposed solution should determine if the cause of performance issues is inside the Java Application, in connected back-end systems or at the network layer.
- The proposed solution should correlate performance data from HTTP Servers (external requests) with internal application performance data
- The proposed solution should measure the end customers' experiences based on transactions
- The proposed solution must be able to proactively identify errors and problems that users are experiencing and enable trouble shooting to begin before an increasing number of users are impacted.
- The proposed solution must be able to pro-actively determine exactly which real users were impacted by transaction defects, their location and status.
- The proposed solution must be able to provide the ability to create user groups based on application criteria or location and link user ids to user names and user groups.
- The proposed solution must be able to provide transaction analysis capabilities and show how a transaction's success rate, average time and transaction count has changed over a specific period of time such as today versus yesterday.
- The proposed solution must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.
- The proposed solution should give visibility into user experience without the need to install agents on user desktops.

- The solution should be appliance-based and deployable as a passive listener on the network thus inducing zero overhead on the network and application layer while monitoring the end-user experience for various web applications hosted in the data center.
- The proposed solution should watch production application components, J2EE services and JVM resources from within the Java / J2EE application with negligible overhead without requiring installation of agents outside the J2EE application server.
- The proposed solution should determine if the cause of performance issues is inside the Java application, in connected back-end systems or at the network layer.
- The proposed solution should provide deeper end-to-end transaction visibility by monitoring at a transactional level.
- The proposed solution should quickly pinpoint the cause of performance bottlenecks through component-level interaction monitoring
- The proposed solution should be able to trace the web transaction components and provide visual representation of an actual transaction if required. All the performance data for the components that make up this transaction should be captured. It should provide an easy way to understand the interaction of the components for e.g. which JSP calls which Servlet or EJB and backend component
- The proposed solution should be able to give a presentation of slowest 'n' calls in the call stack or blame stack.
- The proposed solution should provide fast, automatic discovery and monitoring of the web application environment with zero configurations Out-of-the-box.
- The proposed solution should determine whether web application performance issues are related to the database and collaborate with database administrators so that problems can be detected, isolated and eliminated quickly.
- The proposed solution should quickly isolate web server-related performance problems and effectively communicate with web server administrators for fast problem resolution
- The proposed solution should expose performance of individual SQL statements within problem transactions
- The proposed solution should see response times based on different call parameters
- The proposed solution should shift through thousands of metrics easily and view only the data you care about, thus enabling users to graph and correlate multiple metric values on the fly
- The proposed solution should be JVM & JDK independent, thereby enabling to manage applications on any Java Virtual Machine
- The proposed solution must allow monitoring granularity of no more than 15 seconds for application components and transactions.
- The proposed solution must provide real-time monitoring of key J2EE resources using central agent installed within application:

- JVM memory usage
  - Servlets /JSPs
  - Caches and connection pools.
  - EJBs
  - Struts
  - Socket I/O rates
  - File system I/O rates
  - Method level performance of components monitored
- The proposed solution must proactively count stalled (stuck) threads and monitor thread concurrency by component
  - The proposed solution should share critical application information across the enterprise enabling instant 24x7 monitoring for authorized users anytime, anywhere
  - The proposed solution should view instantly the current value of any metric of any component providing instant real-time performance view
  - The proposed solution should integrate Java application performance data with existing management frameworks.
  - The proposed solution should provide a robust alerting framework and be able to execute one or more notifications and corrective actions e.g. Emails, pop-ups, scripts etc.
  - The proposed solution must have the ability to script actions so that alerts can automatically trigger other processes :
    - Send emails to notify about Alert
    - Turn on transaction tracing
    - Integrate into any SNMP based management or help-desk framework
  - The proposed solution should ensure that historical data is available anytime for problem diagnosis, trend analysis, etc. and can be shared easily with other members of the team
  - The proposed solution should allow data to be seen only by those with a need to know and limit access by user roles
  - The solution should provide an advanced reporting facility with the ability to schedule reports (out of the box and customizable) for any application area.

The proposed **Host-based Server Access Control** solution should be able to protect business critical infrastructure and minimizes security risks by regulating access to confidential business data and mission critical services. The solution should provide policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. Specifically, it should proactively secure access to data and applications located on LINUX/LINUX/UNIX, LINUX/UNIX and Windows system servers throughout the enterprise. The proposed solution must provide the following features:

- Host based security solution must allow controlling of access to all system resources including data files, devices, processes/daemons and audit files.
- The solution should provide OS security hardening and extra levels of access control to the platform.
- The solution should intercept security-sensitive events in real-time, and evaluate its validity before passing control to the OS.
- The solution must be the first layer of security for the system, and any access prevented it should not be overridden by the OS, even if OS permissions directly permit such access.
- The solution should be Non-Intrusive – Must make no changes to the operating system kernel or binaries. Software must allow for quick uninstall if necessary.
- The solution should Self-protect itself – Must be able to prevent hackers with root access from circumventing or shutting down the security engine.
- The proposed solution must use a self-protected database for storing all security information.
- The solution should provide fined grained User Control – Must allow controlling actions and access to resources of all users including privileged accounts such as root / administrator.
- The solution must track the "real user" even in case of surrogates.
- The solution must provide the ability to designate specific users as Administrators, Auditors, and Password Managers etc with appropriate rights. Must also provide the ability to designate specific users as Subordinate or Group Administrators, to manage users and file permissions for their Group
- The solution must support management and policy distribution across Windows, LINUX/LINUX/UNIX and LINUX/UNIX platforms from a central management console. It must support the deployment of the same policies across multiple servers ensuring consistency of security policies across machines in the enterprise.
- The solution must provide simple to use graphical interface to enable complete management of all user, group, resource, audit and policy settings, either centrally for an enterprise or decentralized to departments or business units.
- The solution should be able to specify one rule to apply to many sub-directory trees on system, or have it match a specific filename no matter where it is found on the machine.
- The solution must provide capability to allow access to sensitive resources only through approved programs.
- Administrators must be able to define critical files that are not supposed to change. If these files are modified, the process that checks the sensitive files must find that the files have changed and write an audit record.
- The solution should provide protection against Back Doors and Trojan Horses
- The solution should constantly verify that registered trusted programs are unchanged. If a trusted program is modified, it must mark it as 'un-trusted' and prohibit its execution.

- The solution should provide Process Controls - Administrator must be able to control the circumstances, under which authorized users may terminate sensitive processes (daemons), including time and day, where from, etc.
- Solution must intercept and verify every request to change user identity and maintain a reliable audit trail.
- The user's permissions must always be governed by the original login ID. Even taking over the root account should not grant the user any additional privileges.
- The Solution must enable the administrators to share subsets of root authority among different administrators based on their functional roles.
- The solution should prevent tampering of audit files by anyone while it is running on the machine. Additionally, any change of rules should always be audited.
- The solution should provide firewall-like security by controlling inbound and outbound TCP connections on LINUX/UNIX systems.
- The solution must provide Stack Overflow Protection (STOP) and thereby prevent stack overflow exploits on LINUX/UNIX systems, to ensure that arbitrary commands cannot be executed in order to break into systems.
- The solution should support operating systems such as IBM-AIX, Digital LINUX/UNIX, HP-UX, Sun Solaris, and Windows 2000/2003/2008.
- The solution should provide network source controls – Must be able to restrict user login from specific machines / hosts / terminals for network access or physically connected terminals such as dumb terminals.
- The solution should provide Login controls – Must provide the facility to set accounts to expire on specific dates, deactivate accounts on a configurable date or after a configurable amount of inactive time, lock out accounts after multiple failed logins through a daemon, restrict accounts logins during configurable times and days, deny access to accounts based on company holidays.
- The solution must provide a warning mode that can be used during implementation to verify policies and their impact before deployment.
- The solution should allow protection of files on even non-NTFS file systems like FAT and CDFS.
- The solution should provide a Policy distribution mechanism that is flexible and can be easily applied across domain and platforms.
- The solution should be able to fully work with Win 2K Active Directory in both directions, ensuring any existing deployment of AD infrastructure is not affected.
- The solution should restrict the concurrent logins from one user at any given time, reducing the multiple attacks spawned by some hacking techniques.

- The solution should allow blocking the user login at the local system, and prevent auto-expanding the search across different systems.

**Antivirus Management Solution** should have the following features:

- The solution should protect against all kinds of viruses, Trojan horses and worms including: boot sector, master boot sector, memory resident, file multipartite, macro, stealth and polymorphic
- The solution must scan Floppy disks, CD ROM and Network Drives automatically in real-time when accessed
- The solution must provide a variety of ways to handle viruses, including: cure, rename, move, -report, delete or purge
- The solution must have the capability to automatically copy a file before curing - creating a temporary backup
- The solution must have heuristic scanning to allow rule-based detection of unknown viruses
- The solution must automatically log-off client workstations which attempt to upload an infected file
- The solution must allow administrator to view, configure and manage other NT and NetWare anti-virus servers from a single administrative console
- The solution must automatically discover all machines with antivirus installed. It must collect information such as the OS version, antivirus version, IP address, Mac Address etc.
- The solution must allow grouping of Servers and workstations running antivirus software into hierarchical domains for management and scanning
- The solution must provide a mechanism for developing and distributing policy to each system with respect to scheduling scan jobs, real-time scan settings, signature distribution, alerting and analysis.
- The solution must have support for multiple alerting mechanisms including pager, email, fax notification
- The solution must have options to customize network broadcast intervals, detection heartbeats and server time-outs
- The solution must provide incremental updates rather than distribution of the whole signature each time
- The solution must ensure real time protection even during the signature and engine updating process.
- The solution must support CISCO NAC and Microsoft NAP
- All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security

- Antivirus client must be supported on at least Windows 2000/Windows 2003/ Windows 2008, Windows Vista, NetWare, LINUX/UNIX and LINUX/LINUX/UNIX systems
- The solution must be 100% certified to protect against “in the wild viruses” by the ICSA
- The solution must be industry standard and certified

An **ITIL based Helpdesk system** would be used for assisting the service delivery by Implementation Agency for SDC. Helpdesk system would automatically generate the incident tickets and log the call. Such calls are forwarded to the desired system support personnel deputed by the Implementation Agency. These personnel would look into the problem, diagnose and isolate such faults and resolve the issues timely. The helpdesk system would be having necessary workflow for transparent, smoother and cordial SDC support framework.

- The Helpdesk system should provide flexibility of logging incident manually via windows GUI and web interface.
- The web interface console of the incident tracking system would allow viewing, updating and closing of incident tickets.
- The trouble-ticket should be generated for each complaint and given to asset owner immediately as well as part of email.
- Helpdesk system should allow detailed multiple levels/tiers of categorization on the type of security incident being logged.
- It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.
- It should maintain the SLA for each item/service. The system should be able to generate report on the SLA violation or regular SLA compliance levels.
- It should be possible to sort requests based on how close are the requests to violate their defined SLAs.
- It should support multiple time zones and work shifts for SLA & automatic ticket assignment.
- It should support the holiday definition & SLA clock should stop on holiday or non working days. SLA clock should stop after the analyst shift is over case of non 24x7 support environment.
- It should allow the helpdesk administrator to define escalation policy, with multiple levels & notification, through easy to use window GUI / console.
- It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- It should be able to provide web-based knowledge tools that provides the flexibility to search based on filter noise words methods, list the commonly used security knowledge article methods and deduction methods using a series of questions and answers.

- It should the web-based knowledge tool would allow users to bookmarks their favorite security knowledge articles for quick references.
- It should allow users to rate the usefulness of the knowledge article, so that better and useful articles can be published.
- It should allow the knowledge engineer to create various knowledge categories and assign the documents to these categories.
- It should be possible to specify an expiration date to a document so that if the same becomes irrelevant for an organization it will be unpublished (removed/expired).
- The knowledge tools should provide grouping access on different security knowledge articles for different group of users.
- The proposed system should provide seamless integration to generate events/incident automatically from the existing and proposed NMS and EMS.
- Each incident could be able to associate multiple activity logs entries manually or automatically events / incidents from other security tools or EMS / NMS.
- The proposed system should allow categorization on the type of incident being logged.
- The proposed system should provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels.
- The proposed system should provide an ITIL compliant incident tracking system.
- It should be possible to do any customizations or policy updates in flash with zero or very minimal coding or down time.
- The proposed helpdesk system should provide a built-in workflow engine.
- It should be able to log and escalate user interactions and requests.
- It should support tracking of SLA (service level agreements) for call requests within the help desk through service types.
- It should be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.
- It should provide status of registered calls to end-users over email and through web.
- The solution should provide web based administration so that the same can be performed from anywhere.
- It should have a customized Management Dashboard for senior executives with live reports from helpdesk database.
- The system shall have capability of recording change management information like up gradation/change/replacement of hardware/ configuration details/software added. Any change shall be on cumulative basis with historical information retained.

- It should be possible to attach requests with their corresponding change orders wherever required
- The solution should allow to define complicated workflow tasks with multiple branching and conditions
- The solution should allow these workflow tasks to be assigned to either humans (users) or non human objects like custom java objects, command line process or another workflow instance
- It should allow defining workflow task and attaching the same to the change order category so that the same gets automatically initiated whenever a change order is created with that category.

#### 4.2.1. Directory Services

The configuration of the directory shall depend upon state specific requirements. The directory services shall provide the following features at the minimum:

- Directory Services should be compliant with LDAP v3
- Support for integrated LDAP compliant directory services to record information for users, and system resources
- Should support integrated authentication mechanism across operating system, messaging services
- Should support directory services for ease of management and administration/replication
- Should provide support for Group policies and software restriction policies
- Should support security features, such as Kerberos, smart cards, public key infrastructure (PKI), etc
- Should provide support for X.500 naming standards
- Should support Kerberos for logon and authentication
- Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user
- Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user.

#### 4.2.2. DNS

- Support integration with other network services like DHCP, directory, etc.
- Should support DNS zone storage in Directory
- Should support conditional DNS forwarders e.g. forwarding based on a DNS Domain name in the query.
- Should allow clients to dynamically update resource records secure and non-secure
- Should Support incremental zone transfer between servers

- Should provide security features like access control list
- Should support several new resource record (RR) types like service location (SRV), etc.
- Should support Round robin on all resource record (RR) types

#### 4.2.3. Anti-Virus

- Should restrict e-mail bound Virus attacks in real time without compromising performance of the system
- Should be capable of providing multiple layers of defense
- Should be capable of installation on both the gateway as well as Mailing servers. Inbound and outbound monitoring on all data transfer mechanisms and all e-mail systems
- Should be capable of detecting and cleaning virus infected attachments as well
- Should support scanning for ZIP, RAR compressed files, and TAR archive files
- Should support online upgrade, where by most product upgrades and patches can be performed without bringing messaging server off-line.
- Should use multiple scan engines during the scanning process
- Should support in-memory scanning so as to minimize Disk IO
- Should support Multi-threaded scanning
- Should support scanning of a single mailbox or a one off scan.
- Should support scanning by file type for attachments
- Should support scanning of nested compressed files
- Should be capable of specifying the logic with which scan engines are applied; such as the most recently updated scan engine should scan all emails etc
- Should support heuristic scanning to allow rule-based detection of unknown viruses
- Updates to the scan engines should be automated and should not require manual intervention
- All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security
- Updates should not cause queuing or rejection of email
- Updates should be capable of being rolled back in case required
- Should support content filtering based on sender or domain filtering
- Should provide content filtering for message body and subject line, blocking messages that contain keywords for inappropriate content
- File filtering should be supported by the proposed solution; file filtering should be based on true file type.
- Common solution for anti-spyware and anti-virus infections; and anti-virus and anti-spyware solution should have a common web based management console.

- Should support various types of reporting formats such as CSV, HTML and text files
- Should be capable of being managed by a central management station
- Should support client lockdown feature for preventing desktop users from changing real-time settings
- Should support insertion of disclaimers to message bodies

## 5. KVM

Keyboard, Video Display Unit and Mouse Unit (KVM) and/or other Control Devices/PCs may be used for the IT Infrastructure Management for which the necessary consoles/devices shall be placed by Society for IT Initiatives Fund for eGovernance, Haryana in the location earmarked as Administration Area where the Admin staff will be seated. The KVM unit should provide the following functionalities:

- It should be rack-mountable
- It should have a minimum of 8 ports scalable upto 24 ports.
- It should support local user port for rack access.
- The KVM switch should be SNMP enabled. It should be operable from remote locations.
- It should support a 15 inch TFT monitor with built-in touchpad and a movable front panel.
- It should support multiple operating system
- It should have serial device switching capabilities
- It should have dual power with failover and built-in surge protection
- It should support multi-user access and collaboration

### Technical Specifications:

- AC Power cords, Power Outlet cords, Rack Mounting kit, Software CD, User Manual, Quick Start Guide etc should be supplied as per equipments' requirements.
- Bidder shall only quote for IP KVM solution from brands of ATEN, Altusen, Raritan, Minicomp, & Dell.

### IP KVM on the NET

- Remote access of KVM switches or servers via LAN, WAN, or the Internet
- Multiple user accounts
- Concurrent access to multiple users can log in at the same time
- Message board feature allows logged in users to communicate with other users
- Radius Support
- Browser based access and control
- Windows Client; Java Client for multi-platform support (LINUX/LINUX/UNIX, SUN, etc.)
- Supports TCP/IP, HTTP, HTTPS, UDP, RADIUS, DHCP, SSL, ARP, DNS
- Supports 10Base-T, 100Base-T
- Superior video quality - up to 1600 x 1200
- Advanced security features: 1024 bit RSA; 56 bit DES; 256 bit AES and 128 bit SSL encryption

- Firmware Upgradeable via RJ-45 Ethernet connection
- Remote bootup
- OS Support: Windows 2000, Windows XP, Windows Vista, LINUX/LINUX/UNIX and FreeBSD
- Network Interfaces: TCP/IP, HTTP, HTTPS, UDP, RADIUS, DHCP, SSL, ARP, DNS, 10Base-T/100Base-TX, auto sense, Ping.

#### **IP KVM Control Center Over the NET**

- Complete control of your enterprise – consolidates the management of all ALTUSEN / ATEN IT devices
- Single IP address to securely access every device on the installation
- All devices are integrated into a single tree view for centralized access, administration, and management of a worldwide network from anywhere at anytime
- Web browser access over Internet/Intranet provides secure remote connections to all installed devices
- Windows and Java versions for multiplatform support
- Easy to use – intuitive browser-based GUI for simplified access to IT equipment in global data centers and remote offices
- Scalability – Multi-user access to hundreds of ALTUSEN / ATEN IT appliances and more than ten thousand servers and serially controlled devices
- A single login provides secure, centralized management of multiple data centers, branch offices and remote locations Provides centralized management, Role-Based Access and Control(RBAC), and Reporting Capabilities
- Powerful security features that enable integration with Active Directory external authentication tools
- Robust security policies for individual user authorization to the port level
- 128-bit SSL encryption of all data on the network
- Flexible session time-outs
- "Strong" user name and password authentication
- Network Interfaces allows: TCP/IP, HTTP/HTTPS, SSL, DNS, LDAP/LDAPS
- Powerful portal-like interface provides customized permission-based groupings and device views
- ALTUSEN / ATEN IT appliance auto-discovery with device-availability status, and alarms
- An array of flexible logging and reporting options with audit trails for diagnostics and troubleshooting
- View and manage active user sessions and active ports in real time

- OS Support: Windows 2000 Server/2003 Server/2008 Server/XP, Windows Vista, RHEL AS 4.0 and Fedora Core 4
- Unlimited user accounts can be created
- Capable for Backup LOG DATA and provides also LOG server function
- Should be able to create unlimited user and minimum 10 concurrent users should be allowed.

## 6. Cabling

- CAT 6 / fiber LAN cables should be laid upto the rack level in the Data Centre.
- Dedicated raceways / cable-trays should be used for laying LAN.
- Along with LAN cabling, cables for Storage Area Network (SAN) upto the racks in the Data Centre should also be implemented.
- Cabling for KVM switches on the racks should also be done.
- Additional cabling requirements on an on-going basis will also need to be catered.
- All the cable raceways shall be adequately grounded and fully concealed with covers.
- The cables should be appropriately marked and labelled.

### Technical Specifications:

- Bidder shall only quote for intelligent cabling solutions with successful installation in India
- Intelligent Network Cabling Solution – Hardware

### Detail Specifications:

- The intelligent solution should be based only on a cross connect design to avoid changes directly on the switch ports.
- The Physical Layer Management solution should be based on the PHYSICAL detection of patch cord connectivity ONLY.
- It should monitor all patch panel connections and disconnections
- The intelligent panels should have the necessary intelligent hardware and light indicators integrated in the panels on a per port basis.
- The light guidance (provided by LEDs) is used when tracing two ends of a patch cord. This is required to provide patching information in an easy and straightforward manner. Also this is critical for remote management capability.
- The cross-connect design should be capable to provide solution for reduced patch cords in the communication rooms.
- Scanning devices should be available in 1 U Rack size
- Panels should be available in standard 1U or 2U sizes
- Patch cords are industry standard compliant with one important addition: the patch cords have an internal/external probe which is referred to as the “9th wire” in the patch cord.
- The 9th wire on the patch cords creates a physical circuit connection between the two ports of the panels for correct “physical” connectivity information.
- The Intelligent Physical Layer Management Solution should have the capability to detect automatically and without any human intervention all patch cord connectivity information in following cases:

- If the site is already patched and both the scanning devices & software are installed at a later stage.
- If one or all scanning devices are not working and new patching needs to be done once the scanning devices are functional again
- If one of the patch cords is cut.
- The scanning devices should automatically detect the panel type the scanning devices are connected to and should also automatically detect the connectivity between the scanning devices. This is necessary for automatic & error free detection & installation of hardware components in the software.
- The solution should allow the technician to work without imposing any rules for the patching sequence.
- Since the system, would be used by multiple departments or users, it should provide with an unlimited user licenses.
- The scanning device should be able to monitor panels in more than one rack.

## **Software**

### **Real-Time Monitoring**

- It should automate the process of discovering.
- It should automate the process of documenting
- It should automate the process of monitoring
- It should automate the process of managing the physical networks connections & its devices
- It should have intelligence at physical level to create a topology map at any point in time & to keep track of asset movements.

### **Automatically updates the database:**

- It should report authorized or unauthorized changes in real time

### **Self-Discover Patching:**

- It should self discover all intelligent Management software – enabled port connectivity

### **Event Logs:**

- Whenever the system detects a connectivity change, it should automatically create an entry in an internal comprehensive log.

### **Automated Work Order Process:**

- It should provide a greatly automated work order system, to be shared by the helpdesk, network /telecom managers and technicians.

**Moves Add & Changes (Mac's):**

- Access rights and privileges should be determined by the administrator
- It should allow making MOVES singly or in bulk, as in departmental relocation.
- It should allow authorized users to select the proposed moves of workstations, phones, printers or other equipment.
- It should be capable to include system diagrams and floor plans in the work order.
- It should divide and distribute between various supervisor & technician via email.
- The system should automatically generate auto-routing & a step-by-step work order & schedule, which can be accepted or revised.

**Automatic Re-Synchronization:**

- If a network outage occurs, the Software database should automatically re-synchronize upon the restoration of power, showing network asset connectivity changes.

**Security Features:**

- Software should distinguish unauthorized changes from authorized ones.

**Alerts:**

- It should receive a text message via email containing a predefined message.

**Report:**

- Detailed customizable reports should be provided by the solution

**Auto Routing:**

- The system should automatically generate suggested Auto Routing, and a step-by-step work order and schedule, which can be accepted or revised by the user.

**Utility for Administrator:**

- The solution should provide atleast one utility which can be used by higher management to benefit from the information from the solution without actually directly interacting with the solution. Such a utility should have the capability to analyze information in various formats.

**Rack View:**

- The solution should provide view of rack layout, allow users to view panels in remote and remotely guide technician using the light guidance capability of the intelligent panels.

**Work orders:**

- Provide capability to perform changes through work orders

**Automatic Provisioning:**

- The solution should provide the capability of making movements/changes by simple drag and drop operations. In such situation, the solution should have the capability to automatically suggest patching options and provide work orders

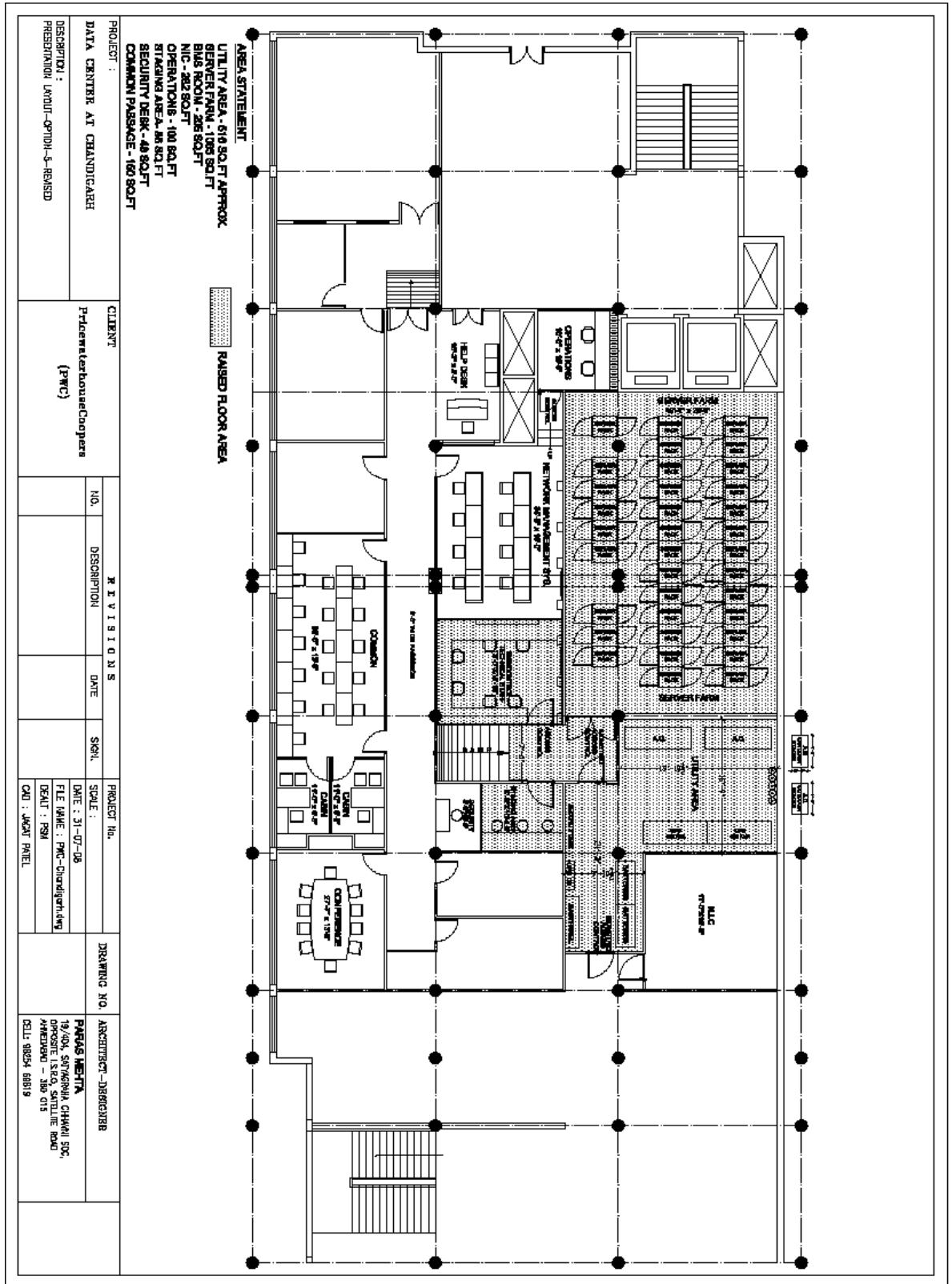
**Offline trouble shooting on network racks:**

- The solution should provide an option to provide to trace ends of patch cords even without communication to the management software.

**Integration with CAD drawings:**

- The solution should provide the option to integrate CAD layouts to enable viewing of devices over CAD.

## 7. SDC Architecture – Physical Infrastructure



**Fig:2**  
 Layout of the site at Mini-Secretariate, Chandigarh

In the schematic above, entire SDC area is logically divided in Zones based MIT guidelines. Each of these zones are having different objective described further in this section. The respective area of each Zone would actually vary, primarily on the basis of number of applications and Size of the State.

- Zone A – This DC Server room area would host servers, server racks, storage racks and Networking component etc.
- Zone B – Comprises of NOC room, reception area, Help Desk area, BMS Area, Testing /Monitoring room etc.
- Zone C – Comprises of room for power panels, AHU, UPS, Fire suppressions, Telecom Room, etc.

A detailed description of key areas of SDC is given below:

### **7.1. Server Farm Area**

The server farm area within the SDC will host / co-locate Intranet Web Servers, Authentication Server, and various Departmental Application Servers including the Database Servers. These servers may be Low end to High-end depending upon the applications hosted on them. These servers may be online or only for repository purpose. The applications, which are running on the central-computing servers, will have load balancing and high availability features.

This area will contain all the networking components from routers, switches to passive components. The data communication component area will terminate SWAN connections, LAN Connections and host a network monitoring station for LAN & WAN. All the Data Center LAN connections will be provided through switches placed in this area.

This area will host the Security components. The security architecture will provide controlled access to the web and database servers from Internet and other networks. This would be multi-layer architecture with two layers of firewall separating the Internet, web, and database/application and Intranet zones.

### **7.2. NOC and Helpdesk Room**

This room will have all the necessary arrangements for the Database, Systems, Application, Authentication and Other Server Administrators. Per shift it is expected to employ one administrator for each of the categories.

SDC shift operators taking care of daily operational activities of SDC will use this area. There will be one Data Center In charge per shift sitting in this area along with shift operators (one each for specific activities like backup, daily Data Center administration / operations etc.)

### **7.3. Backup & Media Storage Area**

This area will be used for storing all backed up Digital Linear Tapes (DLT). This area will house a 3 x 3 x 6 Feet fireproof cabinet for storing roughly 350 tapes. It is also proposed to have an offsite back up where the media tapes will be kept. Presently the Offsite backup is planned in the office of

HATRON in Sector 17, Chandigarh. The offsite backup place will also have a fire and heat proof safe cabinet.

#### **7.4. UPS & Electrical Room**

This area shall house all the Un-Interrupted Power Supply Units and Batteries accompanying this component. As these components generate good amount of radiation it is advised to house these components in a room separate from main SDC room

#### **7.5. Alternative Solution**

The bidder is free to propose an alternative solution for the Haryana State Data Centre than that proposed in this RFP. The alternative solution should be in line with the standard, guidelines provided in the RFP should clearly meet the RFP objectives and the SLA.

#### **7.6. Cost of power and Water during implementation**

It will be the responsibility of the selected bidder to cater to the cost of power and water during the Implementation phase and the cost of the same is inclusive of the implementation cost. However during the O & M, power and diesel costs will be paid by HARTRON on actual on submission of bills.

## 8. Heat Ventilation and Air Conditioning Systems

### 8.1. Air conditioning

Since Zone A is a critical area, a separate air conditioning system (precision air conditioning) should be exclusively installed to maintain the required temperature for Zone A. Zone B & C can have a common air conditioning system for comfort. The general requirements for the two zones are as specified below:

- **Zone A** – should be provided with precision air conditioning on a 24 x 7 x 365 days operating basis at least meeting with Tier – II having n + 1 redundancy at Row level architecture requirements and having enough provision to scale it to next level as may be required in a later stage. The units should be able to switch the air conditioner on and off automatically and alternately for effective usage in pre defined sequence. The units should be down-flow fashion, air-cooled conditioning system. Precision Air Conditioning systems specifically designed for stringent environmental Control with automatic monitoring and control of cooling, heating, humidification, dehumidification and air filtration function should be installed. The heat load calculation & CFD analysis which shows CFM availability on every sever racks in the Data Center should be provided by the bidder as per the details of the racks given at the power requirement. The PAC units shall capable of controlling the CFM & TR capacity with respect to the heat load variations in severs racks to reduce the running cost of Data center on off peak load conditions.
- The SDC should be precision environment controlled. The temperature inside Server Farm area should be maintained at 20 degree centigrade with a precision of  $\pm 1$  degrees and humidity at 50%  $\pm$  5% RH. Air Conditioning **system shall be a floor discharge unit designed specifically for high sensible heat ratio applications such as Server and Computer rooms** should be ensured to the extent of 99.74%. It is suggested to provide adequate air supply typically through false flooring.
- **Zone B/C:** Zone B/C should be provided with split-type comfort air-cooled system ( at least meeting with Tier - II architecture requirements). Help Desk & NOC area should be provided with a separate air conditioning system, so that the air conditioning units can be switched off whenever required.
- The bidder shall carry out design, engineering, manufacture/supply, erection, installation, integration, testing and commissioning of the air conditioning system for the required area indicated in the drawing.
- The bidder shall offer the system that has minimum power consumption to save the operating cost(submit documentary proof on energy saving). Bidder to indicate the power consumption details and means to reduce it to minimum level, without compromising the performance.
- Bidder shall provide clean, controlled and safe environment in all the ambient conditions.

- System shall be designed in such a way that it does not introduce dust, hazardous particles, water particles, smoke, etc. in the environment under any circumstances.
- The air-conditioning system shall be designed specifically for high sensible heat ratio applications like datacenter areas.
- The air-conditioning system should address the specific needs of particular High density sever racks/ units of heat producing hardware in order to achieve a balance psychometric profile.
- Each unit shall be capable of providing sensible cooling capacities at design ambient temperature & with adequate airflow.
- It is essential that the system maintain uniform temperature in all the concerned area, all the time. Design should be such as to avoid hot and cold pockets in racks, (submit documentary proof like CFD / heat capture analysis of the solution).
- The designed system shall have 100% hot stand by redundancy and 20% spare capacity. Normally, all the units shall run in a load-sharing mode. In case of failure of any of the units, others shall take over the total load without affecting the condition of the controlled environment. This should happen seamlessly in minimum possible time.
- The layout of the Data Center is provided in this volume. Bidder shall ensure that the space provided to accommodate the system is adequate. Bidder to make sure that the orientation, opening for Inlet and outlet of airflow, etc. are adequate for the system. Bidder to provide the layout details for the system offered along with design considerations how to achieve the said parameters at rack level.
- Bidder is to design the system that offers minimum maintenance and ease of maintenance. It should be designed in such a way that it is possible to isolate the defective system component and repair / replace without affecting the working of rest of the system
- Manufacturer should have ISO 9001, ISO 14001/ MAIT Level-II Certification

## 8.2. Flexibility

The system should give the flexibility of discharging air at wherever point required even if the furniture is relocated. Changing the grill/tiles carrying grills, at suitable location does this.

## 8.3. Additional Points

- The precision air-conditioners should be capable of maintaining a temperature range of 20 degree with a maximum of 1 degree variation on higher and lower side and relative humidity of 50% with a maximum variation of 5% on higher and lower side.
- The precision air-conditioners shall have 2 independent refrigeration circuits (each comprising 1 no scroll compressors, refrigeration controls and condensers) and dual blowers for flexibility of operations and better redundancy.
- The unit casing shall be in double skin construction for longer life of the unit and low noise level.

- For close control of the SDC environment conditions (Temp. and RH) the controller shall have (PID) proportional integration and differential.
- The precision unit shall be air cooled refrigerant based system to avoid chilled water in critical space.
- The internal cooling design shall follow cold aisle and hot aisle concept as recommended by Ashrae.
- The refrigerant used shall be environment friendly HFC, R-407-C/R-410A equivalent in view of long term usage of the data center equipments, availability of spares and refrigerant.
- For close control of the data center environment conditions (Temp. and RH) the controller shall have (PID) proportional integration and differential.
- The precision unit shall be air cooled refrigerant based system to avoid chilled water in critical space.
- For PAC greater than 10Tr it is recommended that the refrigeration circuit should be dual type, each circuit should have one no of scroll compressor.

#### **8.4. Refrigeration controls, condenser and dual blower**

##### **Requirements:**

- Supply of micro processor based Precision Air conditioning units with environmentally refrigerant gas, each comprising of outdoor and FLOOR DISCHARGE, Top suction indoor unit with Double Skin panels. Outdoor condensing unit shall comprise air cooled condenser with fan speed controller. Outdoor unit shall be an over sized unit to account for high ambient of 45°C & indoor temp. of 20°C, 50%RH. Indoor unit shall consist of filter section, A Microprocessor Controller with LCD Screen, dew point logic & PID Control which is mandatory for controlling & monitoring all the operations of the PAC unit. Electrical Power switch board, multi-rows deep copper cooling coil with aluminum fins, Dehumidification cycle, modular panel cabinet construction, cabinet insulation, fan section with dynamically balanced centrifugal fans with a motor and drive, humidifier, high technology scroll compressor with independent refrigeration circuits, accessible refrigeration control & air discharge duct. The units should have sequencing controller for providing sequencing to the units.
- The unit shall be suitable for 380-440 Volts / 50HZ /3 Phase supply.
- Humidity Control :- 50 ± 5 % RH
- Inside Conditions :- 20 ± 1 Deg C
- Network Interface Card for SNMP/HTTP Connectivity
- The quoted price shall be inclusive of interconnected Copper refrigerant piping up to 10 RMT per circuit including providing support vibration isolation pads and associated electrical cabling up to 10 RMT per circuit between indoor & outdoor units
- The unit shall be suitable for 380-440 Volts / 50HZ /3 Phase supply.

- Supply, installation, testing & commissioning of aluminum Powder coated supply air floor grille with MS volume control damper
- Copper cable interconnection between the outdoor and indoor

## 9. Rodent Repellant

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.

- Configuration : Master console with necessary transducer
- Operating Frequency : Above 20 KHz (Variable)
- Sound Output : 50 dB to 110 dB (at 1 meter)
- Power output : 800 mW per transducer
- Power consumption : 15 W approximately
- Power Supply : 230 V AC 50 Hz
- Mounting : Wall / Table Mounting

## 10. False Ceiling

The top false ceiling would have 10 feet of space from the actual Room ceiling. This false ceiling will house AC ducting (if required) and cables of Electrical lighting, Fire fighting, Rodent Control and CCTV components.

## 11. UPS Requirements & Features

UPS System design concept is based on redundancy and availability, with double conversion true-online system. To support the dual bus system configuration, two units of UPS should be installed. The Zone A area should be having two parallel redundant UPS and other areas like NOC and help desk should have a separate UPS system. Dual redundant UPS systems will take care of following needs –

- Servers
- Access Control / Fire Detection, suppression / surveillance system

The solution should be automatic with power supply from the transformer as the primary source and automatic switchover to DG set as a secondary source for the data centre. Earthing should be provided from the electrical room control panel to the Earthing pits.

It is recommended to have 2 sets of (2 x 160 KVA) UPS with 30 minutes battery back-up on each UPS in Load Bus Synchronization (LBS) configuration. UPS will be preferably supplied power from two different sources. The First set of 2 x 160KVA with each UPS having its own battery bank and Second Set of 2 x 160KVA with each UPS having its own battery bank.

### General Requirements & Design Criteria for the UPS:

- UPS system is required to feed clean and uninterrupted Power Supply to the critical and sensitive load. Power supply system should be designed and engineered such that it enhances the life of the equipment / instruments / computer systems / network devices, etc. installed in the Data Center Facility. It should not under any condition harm the quality of operation of these devices / systems.
- UPS system shall ensure safe shutdown of the systems / equipments / instruments / controls in case of no-mains condition.
- The System shall be designed and integrated with the other Facility systems such that it provides fail safe operations of the systems under no-mains / no-power conditions and /or the abnormal operating conditions such as fire, theft, intrusion, etc.
- Vendor to check and confirm the space available for installation, operation and maintenance of the UPS system including panels, transformers, Distribution Panels / Boards, Batteries, etc. offered.
- The UPS System shall be true on-line, PWM IGBT based, fully double conversion type and of suitable power capacity.

- UPS System shall be with three phase input and three phase output, with proper overload capacity, voltage regulation, transient response, indications, meters, protections, cooling, bypass static switch and remote indication facility.
- The UPS shall have separate battery set having battery back up to support full load of UPS for 30 minutes. The battery set shall be Sealed Maintenance Free (SMF) either Lead Acid category or VRLA type.
- UPS System shall provide regulated and uninterrupted three phase A.C. power, within specified tolerances for deriving power for servers, computers, firewall devices, network equipments and other critical loads during normal and emergency operation.
- The system shall be installed indoor in a clean but hot and humid atmosphere. Precision A/C system shall provide controlled environment during normal operation of A/C system. However, design must consider UPS operation without any deterioration under abnormal atmospheric condition or abnormal condition of A/C system operation.
- UPS system shall be designed for satisfactory and well-coordinated operation with other related equipment as well as input and output systems.
- Energizing or de-energizing any portion of the system serviced by the UPS shall not cause output changes that can affect the operation or integrity of the remaining portions of the system in any way.
- The equipment shall have self-protecting design against all A.C. and D.C. transients, voltage surges, and steady state abnormal voltages and currents.
- The circuit protection shall be coordinated with UPS short circuit capacity and protective device characteristics so that a fault on any circuit shall result in minimum loss of function.
- All non-interrupting components of UPS system shall be capable of withstanding the resultant short circuit current without damage.
- All circuit interrupting components shall be capable of withstanding and interrupting the resultant short circuit currents without damage.
- The charger shall be designed to get maximum life and health (as guaranteed by the battery manufacturer) of the batteries connected to it.
- For continuous operation at specified ratings, temperature rise of the various components of UPS system shall be limited to the permissible values stipulated in the relevant standards and/or this specification.
- It is also recommended to have 2 x 30 KVA UPS with 15 minutes battery back-up for provisioning of the power to the BMS Room, Staging Area and NOC Area.

#### **UPS Modes of Operation**

The UPS shall operate as an ON LINE reverse transfer system in the following modes:

- **Normal** - The UPS inverter continuously supplies the critical AC load. The rectifier / charger derives power from AC Input source and supplies DC power to the Inverter while simultaneously load charging power reserve battery.
- **Emergency** (Failure of AC Input) – Upon failure of AC Input power, the critical AC load will be supplied by the Inverter, which without any switching obtains power from the battery. There shall be no interruption in power to the critical load upon failure or restoration of the AC input source.
- **Recharge** – Upon AC power restoration the rectifier / charger shall automatically restart and assume the inverter and battery recharge loads.
- **Bypass** – A static transfer switch should be provided for performing reverse transfer of the load from the inverter to bypass source with no interruption in the power to the critical AC load. A manually operated maintenance bypass switch should be incorporated into UPS cabinet that will connect the load to AC power source bypassing the rectifier charger inverter and static transfer switch. The battery circuit breaker MCCB shall have O/L and U/V protection. The UPS shall have built in isolation transformer in order to isolate neutral of incoming supply from the load. The load has to be provided separate neutral generated by the secondary winding of output isolation transformer.
- **Paralleling Operations** - The output of all the UPS systems should be directly connected at the load distribution panel through individual circuit breakers (part of the distribution panel). The load at the output should be shared equally by all the UPS systems. The paralleling control mechanism should be available with individual UPS. There should not be any single point of failure which can lead to collapse of all the UPS systems
- UPS shall be connected with LBS (Load bus synchronization system) as recommended by Tier level specifications.
- The transfer of static switch from normal 'Inverter' position to 'stand-by' position shall be initiated by one of the following causes.
  - Inverter failure and UPS system trouble.
  - Inverter output voltage failure.
  - Manual push button operation.
- The static switch shall automatically transfer the load from inverter to stand-by source when the maximum I<sub>2t</sub> capability of the inverter is reached and when the inverter output drops below 90%.
- Transient voltage surge suppression shall be provided at appropriate locations as stipulated by IEEE.
- The power factor of the UPS system should not be less 0.9 and iTHDi <10% at full load conditions
- The battery circuit breaker MCCB shall have O/L and U/V protection.

- PDU with isolation transformer shall be used for power distribution inside the data center if the UPS location is more than 30 metres from the Data center.

### **Battery Requirements**

Battery Bank should be designed to provide 30 minutes back up at full load. Battery should be sealed and maintenance free type. The plates shall be designed for maximum durability during all service conditions including high rate of discharge and rapid fluctuation of load. The UPS Module should have the battery circuit breaker mounted near to the batteries. When this breaker is opened no battery voltage should be present in the enclosure. The battery breaker should be automatically disconnected when the battery reaches to minimum discharge voltage level or when signaled by other control functions. Remote tripping of Battery circuit breaker facility shall be also incorporated. The batteries should be housed in suitable Racks. Battery installation shall be outside the data center area to avoid fire hazard as recommended by NFPA guidelines.

### **Power Distribution**

- Battery installation shall be outside the SDC area to avoid fire hazard as recommended by NFPA guidelines.
- For power transfer from normal to emergency, automatic power transfer switches (ATS) with by pass shall be used as per tier regulations. The ATS shall have overlapping neutral as stipulated by IEEE for electronic switching applications.
- Power cabling inside the SDC shall be of copper. The cables and conduits used inside the SDC shall be of FRLS quality.
- Signal referencing copper earthing to be used using braided copper wire of 6 Gauge inside the SDC.

## **12. Diesel Generator Set**

- The diesel generator set should be in N+1 redundancy mode and total number of units should not exceed three.
- DG Set is required to feed Backup Power Supply to the critical and sensitive load. Power supply system should be designed and engineered such that it enhances the life of the equipment / instruments / computer systems / network devices, etc. installed in the Data Center Facility. It should not under any condition harm the quality of operation of these devices / systems.
- DG Set system shall ensure safe shutdown of the systems / equipments / instruments / controls in case of no-mains condition.
- Vendor to check and confirm the space available for installation, operation and maintenance of the DG Set system including panels, Fuel Tanks, Batteries, etc. offered.
- There should be an Acoustic Canopy / Hood of the appropriate size and as per the norms of the Pollution Control board to suppress the noise of the DG Set to the acceptable level.

## **13. Electrical Work for SDC**

The electrical cabling Work shall include the following.

- Main electrical panel in Data Center
- Power cabling
- UPS Distribution Board
- xUPS point wiring
- Power Cabling for Utility component and Utility Points etc
- Online UPS
- Separate Earth Pits for the component
- The bidder shall insure the power cables and the telephone cables are laid separately and would maintain at least a minimum distance of 2 feet between them so as to avoid electro-magnetic interference

### **13.1. Electrical panel and Distribution boards**

All the Panels shall be metal clad, totally enclosed, rigid, floor / wall mounting, air insulated, cubicle type suitable for operation on three phase / single phase, 415 V / 230 V, 50 Hz., neutral effectively / non-effectively grounded at transformer and short circuit level of 31 MVA.

All the panels shall be IP54 protection class construction.

The Panels shall be designed to withstand a heaviest condition at site, with maximum expected ambient temperature of 50° c., 95% humidity.

The Panels shall comply with the latest edition of relevant Indian Standards and Indian Electricity Rules and Regulations.

The distribution of power from the UPS room to the following shall be considered:

- All proposed component for the production environment
- Existing servers and other component
- Sub distribution panels for UPS
- Final Distribution shall be through Power Distributions Units (PDU)/MCB Distribution Boxes. Power in the racks and other component's shall be provided with two sockets with power coming from separate UPS in each of these sockets. The two UPS power shall be given Static Transfer Switch (STS). All the systems in the rack will be connected to this STS.
- All the Electrical & Power cabling will be terminated in the utility room. The DG related work including the cabling trenching auto synchronization panel would be the responsibility of the selected bidder. Electrical work between auto synchronization panel to the mains would be the responsibility of the selected bidder.

- The bidder shall insure the power cables and the telephone cables are laid separately and would maintain at least a minimum distance of 2 feet between them so as to avoid electro-magnetic interference.
- It will be the responsibility of the bidder to provision the input power from the transformer to the main electrical panel.

**Specifications for Electrical Cabling** –Fire retardant cables of rated capacity exceeding the power requirement of fully blown configuration of the existing and proposed component to be used. For expansion needs suitable redundant power points to be provided at suitable locations. All materials used shall conform to IS standards as per industry practice.

- **Bunching of Wires** – Wires carrying current shall be so bunched in the conduit that the outgoing and return wires are drawn into the same conduit. Wires originating from two different phases shall not be run in the same conduit.
- **Drawing of Conductors** – The drawing Aluminum / Copper conductor wires shall be executed with due regards to the following precautions while drawing insulated wires in to conduits. Care shall be taken to avoid scratches and kinks, which cause breakages.
- **Joints** – All joints shall be made at main switches, distribution boards, socket outlets, lighting outlets and switch boxes only. No joints shall be made inside conduits and junctions boxes. Conductors shall be continuous from outlet to outlet.
- **Mains & Sub-Mains** – Mains & sub-mains wires where called for shall be of the rated capacity and approved make. Every main and sub-main shall be drawn into an independent adequate size conduit. Adequate size draw boxes shall be provided at convenient locations to facilitate easy drawing of the mains and sub-mains. An independent earth wire of proper rating shall be provided. The earth wires shall run along the entire length of the mains and sub-mains.
- **Load Balancing** – Balancing of circuits in three-phase installation shall be planned before the commencement of wiring.
- **Color Code of the Conductors** – Color code shall be maintained for the entire wiring installation, Red, Yellow, Blue for three phases and “OFF” circuit black for neutral and green for earth (or bare earth).
- **Fixing of the Conduits** – Conduits junction boxes shall be kept in position and proper holdfasts shall be provided. Conduits shall be so arranged as to facilitate easy drawing of the wires through them. Adequate junction boxes of approved shape & size shall be provided. All conduits shall be installed so as to avoid stream and hot water pipes. After conduits, junction boxes, outlet boxes & switch boxes are installed in position their outlets shall be properly plugged so that water, mortar, insects or any other foreign matter does not enter into conduit system. Conduits shall be laid in a neat and organize manner as directed and approved by

the Information Technology Department Personnel or person on their behalf. Conductors shall be planned so as not to conflict with any other service pipe lines / ducts.

- **Protection** – To minimize condensation or sweating inside the conductors all outlets of conduit system shall be adequately ventilated and approved by the proper competent authority. All screwed and socketed connections shall be adequately made fully water tight by use of proper jointing materials.
- **Switch-Outlet Boxes and Junction Boxes** – All boxes shall conform to all prevailing Indian Standards. The cover plates shall be of best quality Hylam sheets or ISI grade Urea Formaldehyde Thermosetting insulating material, which should be mechanically strong and fire retardant. Proper support shall be provided to the outer boxes to fix the cover plates of switches as required. Separate screwed earth terminals shall be provided inside the box for earthing purpose.
- **Inspection Boxes** – Rust proof inspection boxes of required size having smooth external and internal Finish shall be provided to permit periodical inspection and to facilitate removal and replacement of wires when required.

## 14. Technical Specifications – Physical Components

### 14.1. UPS

- Input Standard Voltage, 380 /400 / 415 V 3 Phase, 3 or 4 wire, +10 %, -15%
- Input Frequency, 50 Hz, +5% or -5%
- Output Steady State Voltage, 380 / 400 / 415 V +1% or -1%
- Output Frequency, 50 Hz, +0.25Hz to 0.5Hz
- Output Transient Voltage Stability, < 5% or –5% for a load change from 0% to 100%
- Overload – 125% for 10 minutes and 150% for 60 seconds
- Efficiency at full rated load, Not less than 90%
- Total Harmonic Content – With Linear Load < 2% for 100 % linear load and with 3:1 Crest factor load < 5%
- Input Harmonic Filter (for <10% Input current distortion)
- DC ripple (with & without Battery connected) < 1%
- Built In power factor correction
- Automatic shutdown of component for longer power outages
- Monitoring and logging the status of the power supply
- Displaying the voltage/current draw of the component
- Automatic restarting of component following a power outage

- Displaying the current voltage on the line
- Providing alarms on some error connections
- Providing protection against short circuits
- Operating Temperature range - 0 to 40 Celsius, Maximum 50 Celsius for 8 hrs
- Design compliance with IEC and ISO
- Software that must be installed and integrated suitable operating system
- Supplies True Online UPS Power
- Non-Linear load compatible
- Capability to handle high Crest Factor load
- Ventilation- Air cooling with Integral Fans
- Built in Reliability & High Efficiency
- Low Audible Noise
- Compact Footprint
- Front Access for easy Maintenance
- The power factor of the UPS system shall be at 0.9 or better at all load conditions
- Input Current Harmonics < 10%
- The battery circuit breaker MCCB shall have O/L and U/V protection.
- PDU with isolation transformer shall be used for power distribution inside the data center if the UPS location is more than 30 metres from the Data center.

**• Vendor shall submit the efficiency Data of UPS at varying Loads**

Load	25 %	30%	35%	40%	45%	50%	55%	60%	65%	70%	75%	80 %	85%	90 %	95%	100%
Feed 1 UPS																
Feed 2 UPS																

**14.2. Diesel Generator Set**

**Diesel Engine** – Diesel Engine, water cooled, Naturally Aspirated, developing 3 x 300 KVA @ 1500 RPM, under NTP conditions of BS: 5514, with Dry Type Air Cleaner, Compact Radiator with Recovery Bottle and Pusher type Fan, Engine with Coolant, Engine mounted panel with wiring harness, Holset Coupling and Industrial Silencer, as per engine manufacturers design standards.

- **Alternator** – Standard design Alternator, rated at 0.8 PF, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, self-excited and self regulated, with brushless excitation, Self-ventilated, Screen Protected Drip Proof, Insulation Class “H”, enclosure IP 23. The A.C. Generator shall be Horizontal foot mounted single bearing type and shall be fitted with

Automatic Voltage Regulator (AVR) for Voltage regulation of +/- 1% or better. The AVR shall be fitted inside the Alternator terminal box and pre-wired. The Alternator generally conforms to BS: 5000/IS: 4722 and suitable to deliver output of the engine capacity having 750 BHP.

- **Base Frame** – Sturdy, fabricated, welded construction, channel iron Base Frame for mounting the above Engine and Alternator.
- **Control Panel** – Cubicle type, floor mounting Control Panel, with hinged doors, bottom gland plate and accommodating the following:
  - 1-No. ACB or Moulded Case Circuit Breaker suitable to handle the load with O/L, S/C and E/f protection
  - 3-No.'s Ammeters /1 No. Ammeter with Selector Switch
  - 1 No. Voltmeter with Selector Switch
  - 1 No. frequency meter
  - 1 Set Pilot Lamps LOAD ON/GENERATOR ON
  - 1 Set Instrument Fuses
  - The Control panel should be a micro processor based generator set monitoring, metering, protection and control system. It offers advanced levels of functions for reliability and optimum Genset performance. An extensive array of integrated standard control and digital display features eliminate the need for discrete component devices such as the voltage regulator, governor control and protective relays
  - **Battery** – Dry uncharged maintenance free batteries with leads and terminals.
  - **Management**- The DG set should be manageable via Building Management System/ NOC.

#### **ACOUSTIC ENCLOSURE:**

Acoustic Enclosure with other accessories should meet the detailed specifications/ scope of supply as under:

- The noise emission under free field condition shall be 75 dbA at 1mtr. Distance.
- The Acoustic Enclosure should generally comprise / incorporates following:
  - The Structure / Profile should be made out of export quality CRCA Sheet Steel.
  - The roof, side-walls, integral partition and doors should be all sandwich design made out of export quality CRCA Sheet Steel.
  - The Acoustic Enclosure should be natural cooled & maintain  $\Delta t$  (Temp. difference with Air ambient) of 5 - 7° Cent. If need arises articulated ventilation are also considered.
  - The sound absorption material should be selected from either mineral wool / non-igniting foam of relevant thickness and density to meet the performance.
  - The enclosure construction should provide sufficient access for maintenance work.

- The Enclosure should be complete with:
- Arrangement for Power Cable connection for supply to load
- Suction Louvers
- Discharge Louvers
- Openable and lockable doors with Air tight neoprene rubber gasket.
- Interior lighting arrangement - 1 No. Lamp with ON/OFF Switch on Control Panel
- Lifting arrangements

#### **Fuel Tank**

Fuel tank having adequate capacity for each DG set made out of 2 mm thick MS sheet complete with inlet and outlet connections, drain plug, manhole, etc. & suitable for mounting on floor with mounting pedestals. Wire-braided hoses shall also be supplied with fuel tank.

### **14.3. Racks: For housing of all the data center component**

- 40" 42U racks shall be used in the Data Centre for hosting the (HARIS, OTIS, HALRIS & Transport), CSC interface and other department applications of Society for IT Initiatives Fund for eGovernance, Haryana. All the racks should be mounted on the floor with proper floor mounting kits.
- The racks should conform to EIA-310 Standard for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard 19" rack mount equipment.
- Front and Back doors should be perforated with atleast 63% or higher perforations.
- All racks should be OEM racks with Adjustable mounting depth, Multi-operator component compatibility, Numbered U positions, Powder coat paint finish and Protective grounding provisions.
- All racks should have dual power strips, and redundant cooling fan sets.
- All racks must be lockable on all sides with unique key for each rack.
- Racks should also have a provision for cable entry from the top.
- Server Racks should have the following things in addition to the above mentioned hardware
  - Rack mount Keyboard and Monitor
  - USB Interface adapter
  - Serial Interface adapter with power supply
- The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels.
- Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.
- Racks should have Rear Cable Management channels, Roof and base cable access

- Racks should be compatible with floor-throw as well as top-throw data centre cooling systems.
- KVM Switch should be IP based and 1 KVM switch per cluster of racks is required

**Technical Specifications:**

- Network and Server Racks

**Physical Specifications**

- Enclosure dimensions, rack mounting compatibility and weight load ratings:

Internal Height	EIA-310	External Height	External Width	External Depth	Static Rating	Dynamic Rating
42U	19"	1991mm (78.40")	600mm (23.62")	1070mm (42.13")	1364kg (3000lbs)	1023kg (2250lbs)
42U	19"	1991mm (78.40")	750mm (29.53")	1070mm (42.13")	1364kg (3000lbs)	1023kg (2250lbs)

- The 42U unit shall have exterior maximum height measurement of 1991mm (78.40") to allow passage through a standard 2 Meter or 7 Ft. (84") doorway without tipping.
- The 42U units shall support a static load (weight supported by the casters and leveling feet) of at least 1,364 kg. (3,000 lbs.) total installed equipment weight.
- The 42U units shall support a dynamic load (rolling on the casters) of at least 1,023 kg. (2,250 lbs.) total installed equipment weight.
- The units (42U) shall ship with a perforated front door, perforated split rear doors, left and right two-piece solid side panels, tool less roof, four (4) vertical frame posts, four (4) adjustable vertical mounting rails, two (2) vertical PDU mount cable organizers, four (4) leveling feet and four (4) casters, pre-installed by the manufacturer.
- The units (42U) shall ship with baying hardware pre-installed by the manufacturer.
- Baying brackets must provide two sets of mounting holes for standard enclosure spacing of 24" or 600 mm.
- The units (42U) shall ship with grounding hardware pre-installed by the manufacturer.

**Equipment Access & Mounting**

- The unit shall provide 42U of equipment vertical mounting space.
- The vertical mounting rails shall be easily adjustable to allow different mounting depths.
- The vertical mounting rails shall have a second set of EIA mounting holes perpendicular to the primary mounting holes to allow devices to be mounted in the side channel.

- Each vertical mounting rail shall be marked on both sides with lines showing the top and bottom of each U and the number U space next to the middle hole. Each U consists of three square holes and is 1.75 inches (44.45 mm) high.
- The unit shall include at least 60 sets of M6 caged nuts, bolts and cup washers, and caged nut tool for the mounting of equipment inside the unit.
- The manufacturer shall offer an optional hardware kit containing additional M6 caged nuts, screws and cup washers.
- Both the front and rear doors shall be designed with quick release hinges allowing for quick and easy detachment without the use of tools.
- The front and rear doors shall open a minimum of 130 degrees to allow easy access to the interior.
- The front door of the unit shall be reversible so that it opens from either side.
- Split rear doors are provided for increased service clearance.
- The front door of the unit shall be capable of being installed on the rear of the unit, and the rear doors shall be capable of being installed on the front of the unit.
- The unit shall include two-piece removable side panels that are removed without tools using easy finger latches for fast access to cabling and equipment.
- The side panels on the unit shall double as privacy panels when the units are bayed together

#### **Material Requirements**

- All weight bearing components shall be constructed from steel with a thickness no less than 0.9mm (20 gauge).
- All metal parts shall be painted using a powder coat paint process.
- Plastic materials shall comply with Underwriters Laboratory Specification 94 with V-1 rating (UL94 V-1) or better.

#### **Grounding Requirements**

- All enclosure panels and rack-mounted equipment shall be inherently earthed or grounded directly to the frame.

#### **Environmental Requirements**

- The unit shall have a minimum of IP 20 rating for protection against touch, ingress of foreign bodies, and ingress of water.

#### **Safety Requirements**

- The enclosure shall 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.

#### **Ventilation**

- The unit shall provide adequate ventilation to provide airflow required by the major server manufacturers.
- The unit shall provide a minimum total ventilation area for the front door, split rear doors, and roof as specified below
- The unit shall provide the means to mount an optional fan-tray in the roof of the unit and other cooling accessories for high-density.
- The manufacturer shall offer an optional toolless blanking panel kit to prevent the recirculation of hot exhaust air.
- The manufacturer shall offer an optional air baffle kit to prevent the recirculation of hot exhaust air.

### **Security**

- The unit shall include front door lock, rear door lock and side panel lock that are keyed the same; two keys included.
- Replacement key lock cylinders should be available to provide a minimum of 300 unique key combinations on front and rear doors.
- The roof shall not be removable from the interior of the enclosure without tools.
- The manufacturer shall provide optional products and accessories that allow the enclosure environment to be monitored for temperature, humidity, and door access.
- The unit shall have mounting provisions for optional door alarm switch to monitor access to the enclosure doors.

### **Stabilization**

- The unit shall ship with provisions for adding stabilization in the field.
- The manufacturer shall have optional stabilizer plate kit, consisting of a plate, and mounting hardware that can be attached to the enclosure frame, and that can be bolted to the floor.
- The unit shall have mounting provisions for the stabilizer plate on the front and rear (on the interior or exterior) of the unit.
- The manufacturer shall have optional bolt down brackets, consisting of four (4) brackets and mounting hardware that attach to the enclosure frame on the front and rear (on the interior or exterior), and which must be anchored to the sub-floor for compliance with the local Uniform Building Code (UBC).
- The manufacturer should supply structural calculations by a professionally registered engineering firm showing compliance with the local UBC for floor anchoring.
- The unit shall have four (4) adjustable leveling feet to help provide a stable base in the event of an uneven floor surface and to prevent rolling.

### **Packaging**

- The unit shall ship on a wooden pallet. Optional packaging should be available for shipping racks with 1250 lbs and 2000 lbs of installed equipment.
- The unit shall be bolted to the wooden pallet for stability during shipment.
- The unit shall be protected by corrugated corners, which are stretch-wrapped to limit damage during handling.
- The unit shall have a “damage report” sticker on the outside of the packaging which instructs customers to call a toll-free customer support number to resolve possible shipping damage issues.

### **14.4. Jack Panel and Jacks**

The bidder shall provide & configure Jack Panel adhering to international design & quality standards. Cat-6 Patch Cords for patching active connections through Patch Panel shall be offered by the Agency.

## **15. Civil & Architectural work**

The civil work includes furnishing the data center area in all aspects. The furnishing includes but not limited to the following

- Cement Concrete Work
- Cutting and chipping of existing floors
- Trench works
- Masonry works
- Hardware and Metals
- Glazing
- Paint work
- False Flooring
- False Ceiling
- Storage
- Furniture & fixture
- Partitioning
- Doors and Locking
- Painting
- Fire proofing all surfaces
- Insulating

The selected bidder should adhere to the following civil and interior specifications:

### 15.1. Flooring

- Providing and fixing Access flooring system (False floor) HPL panel with edge support rigid grid understructure system. Access floor system to be installed shall provide a maximum finished floor height of 450 mm from the existing floor level. The system shall provide for suitable Floor tiles, pedestals and stringers designed to withstand various static loads and rolling loads. The entire Access floor system shall be made from steel cementations in filled. Access Floor tiles shall provide for adequate fire properties, acoustic barrier and air leakage resistance. The system shall be able to accept an approved laminated floor covering i.e. Anti-static High pressure laminates with PVC beading on the edges of the tiles. the rate shall be inclusive of wire manager & tile lifter etc.
- At least 1' 6" High from existing floor level using antistatic laminated tiles.
- Supply & Fixing of 1.5 mm Antistatic Laminate skirting matching with floor tiles with 8mm thick MDF Board / Bison Board up to a height of 4".
- Supplying and fixing vinyl flooring with homogeneous flexible vinyl flooring of approved shade 2.0 mm thick in roll forms and manufacturers specification over the existing floor. Before laying, the existing flooring should be made free from dust and undulations. The finished flooring should be free from air bubbles and thoroughly cleaned without undulations.
- Providing and laying premium quality Granite white/ cream tiles of size 1'-0" x 1'-0", 8.5 mm thick set in cement mortar and pointing with approved tile joint filler compound of approved make of matching shade as per manufacturer's specification as directed. Rate shall include for preparation of base surface, cleaning, acid wash.
  - do - for skirting upto a height of 4"
- Providing and fixing 9 mm thick floor insulation below the false flooring and joints should be finished properly as per manufacturer's specification. The rate shall be inclusive of cleaning the surface to make it free from dust.

### 15.2. Access Flooring :

- Scope includes providing and fixing access floor system as per the specs in the server room and up to the UPS room including the passage in between. The access floor system to be installed shall provide a minimum finished floor height of 450 mm from the existing floor level. The system shall provide for suitable pedestal and understructure design to withstand various static loads and rolling loads subjected to it in an office / server / DCS / Panel / Rack area. The entire Access floor system shall be consisting of unitized welded steel construction, cementitious filled panel. The Access Floor system shall provide for adequate fire resistance, acoustic barrier and air leakage resistance. The system shall be able to withstand a rated distributed load of not less than 1680kgs and a rated concentrated load of not less than 5.6KN. The understructure should be of rigid grid type and able to accept a pedestal Axial load of not less than 22KN.

- **Ramp:** Providing Ramp at entry points including all supports for the Ramps along with nonskid mats.
- **Lifting devices:** Providing approved panel lifting suction devices for lifting the floor panels

### 15.3. False Ceiling

- Providing and fixing in position gypsum board false ceiling/metal false ceiling with approved G.I./Al/Steel Frame work and hangers including openings for lights etc. to be framed with teak wood members at no extra cost etc. as per specification and description complete.
- Plain horizontal surface.
- Plain vertical surface upto 1' 6" high.
- Providing and fixing 9 mm thick insulation above the false ceiling and joints should be finished properly as per manufacturer's specification. The rate shall be inclusive of cleaning the surface to make it free from dust.
- Providing & fixing of Gypsum FALSE CEILING / Modular false ceiling of 16mm thick tegular edge Diamond Brand™ GRG False Ceiling Tiles of size 600 x 600 mm in true horizontal level suspended on inter locking Diamond Aluminum grid of extruded aluminum sections with powder coating consisting of main "T" runner suitably spaced at joints to get required length and of size 16x32x3600mm made from 1.0mm thick spaced at 600mm center to center and cross "T" of size 16x23x600mm made of 0.10 mm thick. Cross T of 600mm long spaced between main "T" at 600mm center to center to form a grid of 600 x 600 mm and laying 16mm thick GRG false ceiling tiles of approved texture in the grid including, wherever required, cutting/making, opening for services like diffusers, grills, light fittings, fixtures, smoke detectors etc. Main "T" runners to be suspended from ceiling using GI slotted cleats fixed to ceiling with 6 mm dia and dash fasteners, 4 mm GI adjustable rods with galvanized at 1200 mm center to center along main T. Bottom exposed width of 16 mm of all T-sections shall be powder coated with polyester paint All complete at all height as directed

#### **Optional**

- GYPSUM FALSE CEILING ; The rate quoted shall also include making necessary openings/cutouts with required framework in the ceiling for fixing AC diffusers, grills and all type of light fixtures. Paint on the ceiling with plastic emulsion paint as per the specification in the item no. E-1 of paint No separate payment shall be made for grooves, projections, change in level upto any height. The rate quoted shall be applicable for all heights and all type of surfaces i.e. horizontal as well as vertical work shall be done as per drawing. Providing and fixing 12.5mm tapered edge Gypsum board suspended ceiling having the following specifications and satisfying following guidelines for installation as per India Gypsum Co. specification for framework and ceiling.(i) GI perimeter channel of size 20x27x30x 0.5mm shall be fixed on wall to receive ends of ceiling section and outer edge of Gypboard.(ii) M/F

ceiling section of size 51mm and two flanges of 26mm each with lips of 10.50 mm and 0.50mm thick shall be provided at 457mm c/c (max) as main supporting section to fix Gypboard. (iii) Intermediate channel section of size 15x45x0.9mm shall be provided at 1220mm c/c (max) as intermediate support for M/F sections. It shall be suspended from the soffit of RCC slab/beam with the help of ceiling angle of size 25x20x0.5mm provided at 1220mm c/c (max) and fixed to the ceiling with GI soffit cleat of size 22x37mm. Connecting clip of 2.46mm size shall be used to connect the ceiling section to the intermediate channel. 12.5mm tapered edge Gypboard conforming to I.S.2095-1982 shall be fixed to the underside of the suspended grid with the help of screws. Jointing and finishing of the board shall finally be carried out so as to have a smooth, seamless and flush ceiling by using joint tape and jointing compound as per the directions and instructions specified by the manufacturer i.e. India Gypsum Company.

- Provide and Fixing of Armstrong(USA) clip in metal ceiling System on the entire floor consisting of 600x600mm clip in tiles of pre coated galvanized steel in 0.5 mm thickness with bevel edge in white colour with standard perforation of 2.5mm dia & open area of 16%. The back of the tile should have black acoustical fleece of SoundTec make. The NRC should not be less than 0.70 with suitable paint finish and suspension system. The entire ceiling is to be covered with false ceiling.

#### 15.4. Furniture and Fixture

- Workstation size of 2'0" depth made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc complete with French polish. The desk top will be 25mm thick. & edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets, etc. along with sliding / opening as per design, complete with approved quality drawer slides, hinges, locks, etc
- Providing & making of storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate color out side and 2 coat of enamel paint inside the storage of size 1'6"x1'9"x2'4". The rate inclusive of handle, lock, sliding channel and necessary hardware, etc. complete with French polish
- Cabin table of depth 2'-0" made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc complete with French polish.
- Providing, making & fixing 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low ht partition, brick wall, partition wall, cladding etc complete with French polish in all respect.

- Providing, making & fixing an enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate color out side and 2 coat of enamel paint inside the shutter. The rate inclusive of handle, lock, loaded hinges, tower bolt and necessary hardware, etc. complete with French polish.
- Fire proof safe (300 Ltrs or above). It should be 2 hour fire rated.

### 15.5. Partitions

- Providing and fixing in position low height partition wall of 75 mm thick plain gyp-board partition using 12.5 mm thick gyp-board on both sides with GI steel metal vertical stud frame of size 48 mm fixed in the floor channels of 50mm wide to provide a strong partition. Glass wool Insulation inside shall be provided as required. Fixing is by self tapping screw with vertical studs being at 610 mm intervals. The rate shall include making cutouts for switch board, sockets, grill etc. for which no extra will be paid separately The rate shall Include for preparing the surface smoothly and all as per manufacture's specification etc.
- Providing and fixing in position full height partition wall of 75 mm thick plain gyp-board partition using 12.5 mm thick gyp-board on both sides with GI steel metal vertical stud frame of size 48 mm fixed in the floor and ceiling channels of 50mm wide to provide a strong partition. Glass wool Insulation inside shall be provided as required. Fixing is by self tapping screw with vertical studs being at 610 mm intervals. The rate shall include making cutouts for switch board, sockets, grill etc. for which no extra will be paid separately The rate shall Include for preparing the surface smoothly and all as per manufacture's specification etc. Finally finishing with One coat of approved brand of fire resistant coating.
- With Glazing including the framework of 4" x 2" wood section complete (in areas like partition between server & operations & maintenance room and between UPS & G&G workstation areas.).
- Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
- Providing and fixing in position of 75 mm thick plain gyp-board partition using 12.5 mm thick gyp-board on both sides with GI steel metal vertical stud frame of size 48 mm fixed in the floor and ceiling channels of 50mm wide to provide a strong partition. Fixing is by self tapping screw with vertical studs being at 610 mm intervals. Finally finishing with one coat of approved brand of fire resistant coating. The partition will be mainly to clad the shaft walls.
- All doors should be minimum 4 ft wide. Partly / Full glazed 3" thick Sandwiched wood partition with approved shape and shade of finishing as per design and detail of architect using 12 mm thick water proof plywood on both side and using CP Ghana wooden frame work with

lamination to be applied on both sides. Teakwood beading for glass fitting with polishing. All provisions to be made for all electrical, networking, boxes on to partition framework at required heights/levels with necessary additional support as directed.

- Partly / Full partitions made out of Aluminum cross section / 2"x1 1/2" ghanawood section framework 2'-0" c/c both ways treated with anti-termite solution, covered with 6 mm thk ply wood / partly glazed or semi glazed with approved shape & shade of finish as per design and details of Architect. All provisions to be made for all electrical, networking boxes onto partition framework at required heights/levels with necessary additional supports as directed..

### 15.6. Painting

- Providing and applying acrylic plastic emulsion paint of approved make and shade to give an even shade over a primer coat as per manufacturers recommendations after applying painting putty to level and plumb and finishing with 2 coats of plastic emulsion. Base coating shall be as per manufacturer's recommendation for coverage of paint.
- Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.
- Applying approved fire retardant coating on all vertical surfaces, furniture etc as per manufacturer's specification.

### 15.7. Civil Work

- Providing and laying 115 mm thick brick work in cement mortar of 1:4 (1 cement : 4 sand) with bricks of approved quality chamber bricks of class designation 50
- Providing & making SS signage with text in etched & black painted of Dline make or equivalent to be located as directed (wall mounted) for space nomenclature/ directions.
- Plastering with cement mortar 1:5 (1 cement : 5 sand) of 12 mm thick in interior face of the walls and concrete columns including hacking the concrete surface brushing, scaffolding, curing and surface shall be smooth trowel finish as per standard specification.
- Providing & laying 20 mm. thick cement plaster in two coats. First base coat in C.M. 1:4 with rough finishing and second coat in C.M. 1:2 in cement mala finish (finished with steel trowel) including scaffolding, curing, making grooves, forming pattas and drip mould etc. ( Complete at all level )
- R.C.C work: Providing & casting in reinforced cement concrete (M-25) Lintel and RCC band having sufficient reinforcement as per design. Cost to include curing, scaffolding and shuttering. Steel to be considered as 12mm dia @6" c/c placed on both surfaces of slab, wall etc. (If Required)
- Anti-termite treatment in total. Based on actual carpet area. Payment to be paid only on submission of five year warranty certificate from a reputed agency..

### 15.8. PVC Conduit

(Please consider MS pipes, as PVC pipes don't have Fire rating suitable for the Server room applications)

- The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for nonmetallic conduit 1.6 mm thick as per IS 9537/1983.
- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E, regulations for PVC pipes.
- Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.
- The chase in the wall required in the recessed conduit system, shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.
- Field bends shall have a minimum radius of four (4) times the conduit diameter. All bends shall be free of kinks, indentations or flattened surfaces. Heat shall not be applied in making any conduit bend.
  - Conduits and fittings shall be properly protected during construction period against mechanical injury. Conduit ends shall be plugged or capped to prevent entry of foreign material.
- After installation, the conduits shall be thoroughly cleaned by compressed air before pulling in the wire

### 15.9. Wiring

- The bidder shall insure the power cables and the telephone cables are laid separately and would maintain at least a minimum distance of 2 feet between them so as to avoid electro-magnetic interference

- PVC insulated copper conductor FRLS cable / Wires shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 1100 volts grade. Colour code for wiring shall be followed.
- Looping system of wiring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations. No wire smaller than 3.029 sq.mm shall be used.
- Wiring shall be spliced only at junction boxes with ELMEX or CONNECTWELL make terminal blocks having anti-vibration terminals. Maximum two wires can be connected to each way of the terminal block.
- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indicating the circuit and D. B number shall be used for sub main, sub circuit wiring. The ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.
- Separate neutral wire shall be provided for each circuit. Wiring throughout the installation shall be such that there is no break in the neutral wire in form of switch or fuse.
- For lighting fixtures, connection shall be teed off through suitable round conduit or junction box, so that the connection can be attended without taking down the fixture.
- For vertical run of wires in conduit, wires shall be suitably supported by means of wooden/hard rubber plugs at each pull/junction box.
- Normal and Emergency circuits shall not be run in the same conduit.
- Circuits fed from distinct sources of supply or from different distribution boards or M.C.Bs shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to different phase shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.
- Metal clad sockets shall be of dia cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- All power sockets shall be piano type with associated switch of same capacity. Switch and socket shall be enclosed in a M. S. sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live

wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.

- Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts. The earth continuity insulated copper wire in Green colour shall be run inside the conduit to earth the third pin or socket outlets, earth terminal of light fixtures, fan etc. as required. Lights points shall be either of single control, twin control or multiple points controlled by a single switch / MCB as per scheduled of work. Bare copper wire shall be provided with each circuit from DB as specified in the item of work and terminated in earth bar of DBs and switch boxes with proper lugs as required. Maximum number of PVC insulated 650 / 1100 grade copper conductors cable which can be drawn in a conduit.

#### 15.10. Lighting Fixtures

- Fixtures shall be mounted on false ceiling grid with suitable chain and clamps. No cutting or drilling of false ceiling structures is permitted.
- The fixtures after erection shall be marked up indelibly with corresponding circuit number for easy identification of lamp circuit.

#### 15.11. Earthing

All electrical components are to be earthed by connecting two earth tapes from the frame of the component. Ring will be connected via several earth electrodes. The cable armour will be earthed through the cable glands. Earthing shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS- 3843-1986. All the applicable IT infrastructure in the Data Center shall be earthed.

- Earthing should be done inside the Data Centre for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, A.C. units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits.
- EARTH PIT : A pit 2400mm deep of 1000 x 1000mm size, copper plate of 600mm x 600mm x 3mm, sandwiched and buried vertically in alternate layers of salt & charcoal, at the bottom of pit, suitably connected with 3000mm long 25mm x 3mm copper strip laid upto the ground level, 15mm dia perforated GI pipe with funnel at top for watering, masonry chamber of clear inner dimensions of 300mm x 300mm x 300mm size with CI cover; including all necessary hardwares & accessories complete as per IS 3843.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.

- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 2.5 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.
- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.
- The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic earthing measurements should be available on the UPS panel itself in the UPS room.
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
- The grounding shall be done by G.I. flat/ copper/ AL conductors of sizes as laid down in grounding drawings and the same shall be connected to the risers of main ground mat.
- In case of site fabricated cable tray/ladder, the runner angles shall be used as ground conductors and shall be made electrically continuous.
- All ground conductor connections shall be made by electric arc welding/brazing unless otherwise specified. Ground connections shall be made from nearest available station ground grid risers.
- All ground conductors WELDED/BRAZED connection shall be painted black for prevention of corrosion.
- Equipment will generally be furnished with two separate ground pads with tapped holes, bolts and spring washers. If, however, the same are not furnished, Contractor shall drill and tap holes and provide bolts, spring washer for connection.
- Equipment ground connections, after being checked and tested by the Engineer, shall be coated with anti-corrosive paint.
- Whether specifically shown or not, all conduits, trays, cable armour and cable end box, electrical equipment, such as motors, switch boards, panels, cabinets, junction boxes, lock-out switches, fittings, fixtures, etc. shall be effectively grounded.
- All equipment, supporting steel structures, panels, boards, switchgears, junction boxes, conduits, etc. shall be grounded in compliance with the provision of I.E. Rules.
- All ground connections shall be made from nearest available station ground grid. All connections to ground grid shall be done by arc welding unless otherwise stated.

### 15.12. Cable Work

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct .Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required Cables shall be neatly arranged on the trays in such manner that a crisis crossing is

avoided and final take off to switch gear is easily facilitated.

- All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick aluminum strips and securely fastened to the cables at both the termination ends. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.
- Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.
- Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.
- Prior to laying of cables inside both indoor and outdoor trenches, the contractor shall properly clean inside those trenches.
- In outdoor areas, buried cables shall be laid and covered with sand/riddled earth and protected from damage by bricks at sides and precast slab at top.
- When buried cables cross road/railway track, additional protection shall be provided in the form of Hume / galvanized iron pipes.
- For buried cable, the marker shall project 150 mm above ground and shall be spaced at an interval of 30 metres and at every change of direction.
- The termination and connection of cables shall be done strictly in accordance with manufacturer's instruction, drawings and/or as directed by the Engineer.
- The work shall include all clamping, fitting, fixing, cable jointing, crimping, shorting and grounding etc. as required for heat/cold shrinking technology for the complete job. All equipment required for all such operations shall be of contractor's procurement under this specification.
- All cable entry points shall be properly sealed and made vermin and dust-proof. Unused / spare opening, if any, shall be effectively closed. Sealing work shall be carried out with approved sealing compound having fire withstand capability for at least three hours.
- Cable shall be installed without joints as far as practicable.
- If, however, jointing becomes necessary, it shall be made only by qualified cable jointer and strictly in accordance with manufacturer's recommendation.
- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.
- Necessary earthing arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends.

The rising mains enclosure shall be bolted type.

- The total no of ports for data and voice will be finalized by the selected bidder in concurrence with HARTRON after finalization of working drawings layout.

## 16. Fire Detection and Control Mechanism

### System Description

- The Fire alarm system shall be an automatic 1 to n (e.g. 24) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.
- Detection shall be by means of automatic heat and smoke detectors located throughout the Data Center (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

### Control and indicating component

- The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.
- All controls of the system shall be via the control panel only.
- All site-specific data shall be field programmable and stored in an integral EEPROM. The use of EPROM's requiring factory 'burning' and re-programming is not acceptable.
- All internal components of the control panel shall be fully monitored.
- The control panel shall be capable of supporting a multi device, multi zone 2-wire detection loop. Removal of 1 or more detection devices on the loop shall not render the remaining devices on the loop inoperable.
- The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.
- All user primary controls shall be password protected over 4 access levels in accordance with EN54 Part 2. Essential controls, such as Start / Stop sounders and Cancel fault buzzer, etc. will be clearly marked.
- Cancel fault and display test functions shall be configurable to be accessed from level 1 or level 2.
- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
- The control panel shall log a minimum of 700 events comprising of 100 event fire log and 200 event fault, disablement and historic logs, giving time, date, device reference and status of indication.
- Fire, fault and disablement events shall be logged as they occur. Visual and audible conformation shall be given on an array of LEDs, the Liquid Crystal Display and the internal supervisory buzzer.
- The control panel shall have an integral automatic power supply and maintenance free sealed battery, providing a standby capacity of a minimum 72 hours and further 30 minutes under full

alarm load conditions. The system shall be capable of full re-charge within 24 hours following full system discharge. The performance of the power supply and batteries shall be monitored and alarm rose, should a fault be detected. The system shall protect the batteries from deep discharge.

- All terminations within the control panel with the exception of the 230V mains connection will be via removable terminal screw fixing points.
- The control panel will have a programmable maintenance reminder to inform the user that maintenance of the system is required. This function shall provide the user with the option of a monthly, quarterly, annually or bi-annually reminder prompts. The maintenance reminder will be indicated on the control panel. This message shall be resettable by the user and will not require the intervention of specialist support. The control panel will provide programmable free text field as part of the maintenance reminder facility.
- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.

### **Manual Controls**

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Enter or modify device text label
- Setup maintenance reminder
- Assign or modify zones
- Disable zones, device, sounders, FRE contact, auxiliary contacts
- Enable zones, device, sounders, FRE contact, auxiliary contacts
- Action weekly test
- Disable loop

**Cable entries** – The control panel will include the necessary top entry and rear entry cable entry points via 20mm knockouts.

**Manual call points (MCP)**

- MCP's shall be addressable and of the steady pressure break glass type manufactured to the requirements of BS 5839: Part 2. A test key shall be provided to allow the routine testing of the unit to meet the requirements of BS 5839 Part 1 1988, without the need for special tools or the need to unfasten the cover plate.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches. The device shall incorporate a short circuit isolation device and a red LED indicator.
- The MCP shall be suitable for surface or flush mounting. When flush mounted the device shall be capable of fixing to an industry standard single gang box.

**Smoke detectors** – Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

**Heat detectors**

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved.
- The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

**Addressable detector bases**

- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

**Audible Alarms** – Electronic sounders shall be colored red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

**Commissioning**

- The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.
- The labeling of Device and Zone labels should be part of the system.

- Necessary Software to the control panel

### **16.1. Fire Suppression System**

- Fire suppression system shall deploy FM-200 (ETG-5) based gas suppression systems with cross-zoned detector systems for all locations. These detectors should be arranged in a manner that they activate the suppression system zone wise to cater to only the affected area.
- There should be a fail-safe alarm system to prevent false discharge or tampering.
- Additionally, Portable Extinguishers (CO2 or Helotron. Halon based Extinguishers are not acceptable) shall be placed at strategic stations throughout the Data Centre.
- Bidder should provide dual interlock pre-action dry pipe fire suppression systems.
- Illuminated Signs indicating the location of the extinguisher shall be placed high enough to be seen over tall cabinets & racks across the room. Linear heat detection cable should be placed along all wire pathways in the ceiling. This should not directly trigger the suppression system—rather; it should prompt the control system to sound an alarm.

#### **Mandatory Bidding Requirements**

- The OEM (/ Bidder) shall give a Certificate stating that their FM-200 system is approved by UL / FM / VdS / LPC/CNPP for use with Seamless Steel Cylinders (Component as well as System Approval).
- The OEM (/ Bidder) shall also provide a Letter that the OEM has FM-200 Flow Calculation software suitable for Seamless Steel cylinder bided for as per the Bill of materials and that such Software shall be type approved by FM / UL / VdS / LPC.

#### **Specific Technical Requirements**

- The Storage Container offered shall be of Seamless type, meant for exclusive use in FM- 200 systems, with VdS/FM/UL/LPC/CNPP component approval. Welded cylinders are not permitted.
- The Seamless storage cylinder shall be approved by Chief Controller of Explosives, Nagpur and shall have NOC from CCoE, Nagpur for import of the same. Documentary evidence to be provided for earlier imports done by the bidder.
- The FM-200 valve should be Differential Pressure Design and shall not require an Explosive / Detonation type Consumable Device to operate it.
- The FM-200 Valve operating actuators shall be of Electric (Solenoid) type, and it should be capable of resetting manually. The Valve should be capable of being functionally tested for periodic servicing requirements and without any need to replace consumable parts.
- The individual FM-200 Bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure.

- The system flow calculation be carried out on certified software, suitable for the Seamless Steel Cylinder being offered for this project. Such system flow calculations shall be also approved by VdS / LPC/ UL / FM.
- The system shall utilize 42 Bar / High pressure (600 psi) technology that allows for a higher capacity to overcome frictional losses and allow for higher distances of the agent flow; and also allow for better agent penetration in enclosed electronic equipments such as Server Racks/ Electrical Panels etc.
- The designer shall consider and address possible Fire hazards within the protected volume at the design stage. The delivery of the FM-200 system shall provide for the highest degree of protection and minimum extinguishing time. The design shall be strictly as per NFPA standard NFPA 2001.
- The suppression system shall provide for high-speed release of FM-200 based on the concept of total Flooding protection for enclosed areas. A Uniform extinguishing concentration shall be 7% (v/v) of FM-200 for 21 degree Celsius or higher as recommended by the manufacturer.
- The system discharge time shall be 10 seconds or less, in accordance with NFPA standard 2001.
- Sub floor and the ceiling void to be included in the protected volume.
- The FM-200 systems to be supplied by the bidder must satisfy the various and all requirements of the Authority having Jurisdiction over the location of the protected area and must be in accordance with the OEM's product design criteria.
- The detection and control system that shall be used to trigger the FM-200 suppression shall employ cross zoning of photoelectric and ionization smoke detectors. A single detector in one zone activated, shall cause in alarm signal to be generated. Another detector in the second zone activated, shall generate a pre-discharge signal and start the pre-discharge condition.
- The discharge nozzles shall be located in the protected volume in compliance to the limitation with regard to the spacing, floor and ceiling covering etc. The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final number of the discharge nozzles shall be according to the OEM's certified software, which shall also be approved by third party inspection and certified such as UL / FM / VdS / LPC.
- FM-200 shall be stored in seamless storage containers complying with the SMPV Rules set out by Chief Controller of Explosives, Nagpur, India. The Bidder shall be required to produce a NOC for the Chief Controller of Explosives, Nagpur for the storage containers against the cylinder identification numbers punched on them.
- Welded cylinders for agent storage will not be acceptable – NOR shall be such Seamless cylinders & Cylinder manufacturers, that do not already have the approval of Chief Controller of Explosives, Nagpur.

- The Cylinder shall be equipped with differential pressure valves and no replacement parts shall be necessary to recharge the FM-200 containers.
- FM-200 shall be discharged through the operation of an Electric (solenoid) operated device or pneumatically operated device, which releases the agent through a differential pressure valve.
- Systems that employ explosive or pyrotechnic devices for FM-200 discharge shall not be permitted.
- All system components shall be New and of Current manufacture and shall be installed in accordance with local codes.
- The suppression agent shall be UL component recognized
- The bidder shall provide all documentation such as Cylinder Manufacturing Certificates. Test and Inspection Certificates and Fill Density Certificates.

The extinguishing system shall include the following components:

- Agent storage container with cylinder valve, pressure gauge, Low-pressure Switch
- FM-200 agent
- Discharge nozzle(s)
- Solenoid valve(s) and Pneumatic Actuator(s)
- Manual Actuator(s)
- Mounting brackets
- Discharge hoses
- Check valves
- Inter-connecting Actuation hoses
- Manifolds and piping with fittings
- Any other required for the completeness of the system
- The FM-200 discharge shall be activated by an output directly from the 'FM-200' Gas Release control panel, which will activate the solenoid valve. FM-200 agent is stored in the container as a liquid. To aid release and more effective distribution, the container shall be super pressurized to 600 psi (g) at 21°C with dry Nitrogen.
- Cylinder valve bodies shall be brass. Any other materials of construction shall not be acceptable.
- The releasing device shall be easily removable from the cylinder without emptying the cylinder. While removing from cylinder, the releasing device shall be capable of being operated, with no replacement of parts required after this operation.

- Upon discharge of the system, no parts shall require replacement other than gasket, lubricants, and the FM-200 agent. Systems requiring replacement of disks, squibs, or any other parts that add to the recharge cost will not be acceptable.
- Systems containing components that have a dated life span and must be periodically replaced shall not be acceptable.
- The releasing of FM-200 Cylinder(s) shall also be possible through direct mechanical actuation, providing a means of discharge in the event of total electrical malfunction.
- The manual release device fitted on the FM-200 Cylinder(s) shall be of a manual lever type and a faceplate with clear instruction of how to mechanically activate the system. In all cases, FM-200 cylinders shall be fitted with a manual mechanical operating facility that requires two-action actuation to prevent accidental actuation.
- FM-200 storage cylinder valve shall be provided with a safety rupture disc. An increase in internal pressure due to high temperature shall rupture the safety disc and allow the content to vent before the rupture pressure of the container is reached. The # contents shall not be vented through the discharge piping and nozzles.
- FM-200 containers shall be equipped with a pressure gauge to display internal pressure.
- Brass Discharge nozzles shall be used to disperse the `FM-200`. The nozzles shall be brass with female threads and available in sizes as advised by the OEM system manufacturer. Each size shall come in two styles: 180° and 360° dispersion patterns.
- The nozzles provided shall be UL listed or VDS/LPC approved.
- All the Major components of the FM-200 system such as the Cylinder, Valves and releasing devices, nozzles and all accessories shall be supplied by one single manufacturer under the same brand name.
- Manual Gas Discharge stations and Manual Abort Stations, in conformance to the requirements put forth in NFPA 2001 shall be provided.
- Release of FM-200 agent shall be accomplished by an electrical output from the FM- 200 Gas Release Panel to the solenoid valve and shall be in accordance with the requirements set forth in the current edition of the National Fire Protection Association Standard 2001.

**Acceptance Tests:**

- Acceptance for the System installation, inclusive of the piping and requisite cabling shall be strictly in accordance with the installation acceptance guidelines as put forth in the NFPA 2001. The bidder shall be required to carry out a simulation test [with the Electrical Solenoid on the FM200 bank (/ Cylinder) disabled / disengaged so as to prevent discharge of gas], and prove the functionality of the System.
- Gas dump test is outside the purview of this specification, due to commercial considerations, and as the guidelines put forth by NFPA 2001.

## 16.2. System consideration and requirements

### System Drawings:

- The Bidder shall specifically prepare plans, which are to an indicated scale with lettering no smaller than one-eighth inch and easily reproducible. These plans will show the quantity, location, and marking of all system components. Included shall be a description and routing of all piping.
- Computer flow calculations using the manufacturers approved software shall detail pressure changes, flow rates, pipe and nozzles sizes.
- Care should be taken to locate all agent storage containers as close to the protected area as possible to ensure complete liquid discharge of the suppression agent within 10 seconds. System electrical schematics and diagrams shall be provided, including a description of all interlock functions.

### Codes and Standards

- NFPA 2001 standard on Clean Agent Fire Extinguishing System
- Clean agent manufacturers recommendation

## **17. Air conditioning system**

The SDC shall be provided with fully redundant Microprocessor based Precision Air-conditioning system using redundant Air Handling Units (AHU) & Chillers. Cool air feed to the SDC shall be bottom-charged or downward flow type using raised floor as supply plenum using perforated aluminum tiles for Air flow distribution. The return air flow shall be through ducts on false ceiling to cater to the natural upwardly movement of hot air. Cooling shall be done by the Air-conditioning system only. Forced cooling using Fans on False floor, etc is not acceptable. The following points must be addressed by the air conditioning system:

### **a. Temperature requirements**

The environment inside the SDC shall need to be continuously maintained at  $20^{\circ} \pm 1^{\circ}$  Centigrade. It is advised that the temperature and humidity be controlled at desired levels. The necessary alarms for variation in temperatures shall be monitored on a 24x7 basis and logged for providing reports.

### **b. Relative Humidity (RH) requirements**

Ambient RH levels shall need to be maintained at  $50\% \pm 5$  non-condensing. Humidity sensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24x7 basis and logged for providing reports.

### **c. Temperature & Relative Humidity Recorders**

Temperature and Relative Humidity Recorders shall preferably be deployed for recording events of multiple locations within the SDC. Records of events for about past 7 days shall be recorded and presentable whenever required by Society for IT Initiatives Fund for eGovernance, Haryana. Automatic recording of temperature and humidity using sensors located at various locations within the SDC is necessary.

### **d. Air quality levels**

The SDC shall be kept at highest level of cleanliness to eliminate the impact of air quality on the hardware and other critical devices. The SDC shall be deployed with efficient air filters to eliminate and arrest the possibility of airborne particulate matter which may cause air-flow clogging, gumming up of components, causing short-circuits, blocking the function of moving parts, causing components to overheat, etc. Air filters to provide up-to 5 Micron particulate shall be deployed. The allocated area shall be vacuum-cleaned on a regular basis in consultation with Society for IT Initiatives Fund for eGovernance, Haryana representatives.

### **Precision air conditioning system for Zone A:**

- The system shall contain Scroll compressor, Evaporator, Humidifier, Condenser and an Externally Equalized Thermostatic expansion valve (TXV) all of which shall be contained within the cabinet of the unit.
- All electrical wires / cables used across all units should be FRLS.

### **Cabinet Construction**

- The cabinet should be constructed from best quality sheet steel of thickness not less than 1.6 mm (16 gauges) thick suitably treated for weather protection, corrosion and shall be powder coated.
- Sandwich panel construction with CCF / Fire retardant grade insulation (25 mm thick) on all sides to reduce noise level in the room.

#### **Evaporator Section**

- Evaporator Coil
- Coil should be single but there should be two independent refrigeration circuits with separate blowers and condensers to have inbuilt redundancy as the capacity is high.
- Evaporator coil should be constructed out of copper tubes not less than 0.345 mm thick expanded on to aluminum fins to give a good mechanical bond for maximum heat transfer. Approximately 12 numbers of fins per inch should be provided. Fin thickness should not be less than 0.12 mm.
- Face area of coil should be selected corresponding to air velocity not exceeding 2.5 m / sec.
- A condensate drip tray of powder coated construction of minimum 18 SWG thick along with a Special plastic pipe to drain out condensate water should be provided.

#### **Compressor**

The compressor shall be of high efficiency SCROLL design, with an E.E.R. of not less than 11.0 BTU/Watt. Compressor shall have inbuilt overloads, and shall be mounted on anti vibration mountings.

#### **Refrigeration circuit**

- The refrigerant circuit should be suitable for operation of R-407 and should include the following items :
  - Thermostatic Expansion Valve with external Pressure equalization
  - Removable liquid line drier / filter
  - Liquid Line Sight Glass with Moisture indicator
  - Hand shut of valve
- Suction and discharge valves for isolation of Compressor
- There should be two independent refrigeration circuits with separate blowers and condenser assembly.
- The serviceable / removable components should have union connections for easy removal / assembly.

- All pipe works should be carried out with refrigerant quality copper tubes and where bends are required these should be completed using either a proprietary bending tool or radius fittings. The minimum thickness of pipe should be 1.6 mm (16 SWG).

**Fan Motor Assembly:**

- Fan should be driven by a weather proof TEFC Motor suitable for operations on 415 +/- 10% variations 3 phase, 50 Hz AC supply. The motor housing shall be of IP 22 grade.
- The fan should be belt driven having a maximum speed of 1400 r.p.m.
- Energy efficient motors as per IS 12615 of 1989 should be used.

**Humidifier**

- Humidification shall be provided by boiling water in a polypropylene steam generator. The steam shall be distributed evenly into the bypass air stream of the precision air-conditioning unit. The humidifier shall be capable of providing 7.5 kg of steam per hour. The humidifier shall have an efficiency of not less than 1.3 kg per kW and be fitted with an auto flush cycle activated on demand from the unit's control system.
- The humidifier shall be fully serviceable with replaceable electrodes. Waste water shall be flushed from the humidifier by initiation of water supply solenoid valve via a U pipe system.

**Electrical heating**

- The electrical heating elements shall not operate at a level exceeding 60 W/Sq. m. The low watt density elements shall be of finned tubular construction. The total heater capacity should not exceed 9 Kw.
- The heating circuit shall include dual safety protection through loss of air and high temperature controls.

**Service Area**

- The unit shall be serviceable with a maximum service space of 600mm in front of the unit.

**Air Filtration**

- High efficiency EU-4 filters located on the air inlet face of the cooling coil. The filter media should be fire retardant.

**Air-cooled condensers**

- For each packaged air conditioner unit there should be one air cooled condenser unit, having a matching heat rejection duty.
- The condenser unit should incorporate the following :
- The condenser coil should not be less than 0.355 mm (29 G). Approx. 12 FPI shall be provided.
- Two fans shall be provided for each condenser unit and should be selected for low speed quiet operation. The fan should be directly driven by an energy efficient motor of speed not exceeding 1000 R.P.M and constructed from sheet and cast aluminum.

- The condenser should be vertical mounting type with horizontal throw of air, having suck through arrangement ensuring even air flow over the coil block, optionally or side throw or top throw.
- All the foregoing items should be factory assembled with body made out of 1.6 mm (16 SWG) M.S. Sheet (Powder Coated).
- The entire assembly should be supported by a corrosion treated frame.
- Fan motor should be provided with VSD to modulate as per ambient temperature conditions and also as per operating load pressures.

### **Controls**

Following controls should be provided:

- High pressure trip – Manual reset (for each compressor)
- Low pressure trip – Manual reset (for each compressor)
- The thermostat and humidistat to control operation of the unit
- Single phase preventer.
- Reverse Phasing
- Phase Failure

### **Safety Interlocks**

- Interlock between condenser fan motor and compressor motor to prevent starting of compressor without condenser fan in operation
- Condenser fan should stop along with compressor
- Provision should also be made to operate the evaporator fan without the operation of condenser and compressor
- Time delay of minimum three minutes shall be there for restart of compressor
- Operation of heaters & humidifiers shall be possible only when blower fan is in operation.
- Fire detection signal from fire detector system shall be able to switch off the package unit operation in event of fire in conditioned space.

### **Controller**

- Microprocessor based programmable logic controller fully compliant with EEC directives for electromagnetic compatibility with following broad features:
- Operates monitors and displays so that the room temperature and humidity is kept at  $20 \pm 1$  Deg C and  $50\% \pm 5\%$  RH respectively.
- Password protected for authorized access alone.
- User friendly interface with backlit LCD screens that indicate through animation and icons plant items (Actual and set point temperature and humidity etc) history of alarms, alarms logging (High temperature, compressor HP / LP, low humidifier water, overload, air flow failure, dirty filter etc).

- Allows adjustment of temperature and humidity set points, range of control, alarm set points, etc.
- Auto time sharing – Ensures are units run on equal number of hours
- Arrow / control buttons for navigation and value adjustment.
- Status indicators like power, cool, humidity etc

Following features should be given by the microprocessor:

- Room temperature and humidity.
- Supply fan working status.
- Compressor working status.
- Electric heaters working status.
- Manual / Auto unit status.
- Temperature set point.
- Humidity set point.
- Working hours of main component i.e. Compressor, fan, heater, humidifier.
- Unit working hours.
- Current date and time.
- Type of alarm (with automatic reset or block)
- The last 10 intervened alarms.

The Microprocessor shall be able to perform following functions:

- Testing of the working of display system.
- Password for unit calibration values modification.
- Automatic reset of program.
- Cooling capacity control.
- Compressor starting timer.
- Humidifier capacity limitation.
- Date & time of last intervened alarm.
- Start / Stop status storage.

Following alarms shall be displayed on screen of microprocessor unit:

- Airflow loss.
- Compressor low pressure.
- Compressor high pressure.

- High / low room temperature.
- High / low room humidity.
- 2 spare external alarms.
- Wet floor.

## 18. High Sensitivity Smoke Detection System

**General** – The HSSD system shall provide a early warning of fire in it's incipient stage, analyze the risk, and provide alarm and actions appropriate to the risk The system shall include, but not be limited to, a Display Control Panel, Detector Assembly, and the properly designed sampling pipe network. The system component shall be supplied by the manufacturer or by its authorized distributor.

### **Regulatory Requirements**

- National Electrical Code (NEC)
- Factory Mutual
- Local Authority having Jurisdiction

## 19. Access Control System

- An access control system consisting of a central PC, intelligent controllers, proximity readers, bio-metric finger print reader, power supplies, proximity cards, and all associated accessories is required to make a fully operational on line access control system including all required database management, configuration software, database storage system software and hardware, as well as complete browser based Access Control and Alarm Monitoring software package including a dynamic and interactive graphical user interface.
- Access control shall be provided for doors. These doors shall be provided with electro magnetic locks, and shall operate on fail-safe principle.
- The lock shall remain unlocked in the event of a fire alarm, or in the event of a power failure.
- The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors.
- Entry to the restricted area shall be by showing a proximity card near the reader / bio metric finger print reader and exit shall be using a proximity card reader / push button installed in the secure area.
- The system shall monitor the status of the doors through magnetic reed contacts.

**The Security Access Control System shall provide the following card access control operational objectives:**

- Controlled entry, via access card readers, of only authorized personnel to secured areas based on cardholder information entered and stored in the system database.
- The access request response time from card presentation, database verification, to electric lock unlock shall be no more than one second in normal operating mode on a fully loaded system.

- All access requests, both authorized and denied, shall be sent to the host for storage and annunciation, as required, with the cardholder number, name, and access point/area where access was attempted or gained.
- The software package shall provide for Local Anti-Passback, and also provide a facility for “soft” Anti-Passback (i.e. allowing entry following an Anti-Passback violation but still report and log the violation.) The system shall also be capable of providing timed Local Anti - Passback for security areas
- The system shall provide for automatic lock/unlock of access-controlled doors on a scheduled basis using time schedule.
- Each card and cardholder shall be entered into the database prior to their use. Each card can be manually disabled at any time without the requirement to delete the card. Each card can then be subsequently re- enabled at a later time.
- Card records shall include the entry of activation and deactivation dates to provide for the automatic enabling and expiring of the card record.
- The operating mode of access controlled doors shall be indicated as locked, unlocked, or controlled. The door status shall be indicated as open or closed.
- The system shall provide for the monitoring of the reader controlled door position in order to detect and report Door Forced Open and Door Held Open alarm conditions. Door Held Open condition shall be based on a user-adjustable time period. The act of opening the door shall initiate the door timer, and also cause the immediate reset of the door lock.
- The system shall provide for the designation of certain calendar days to be holidays, with special access privileges and system activity to be specified for those days.
- The system shall provide the capability to unlock the door and/or mask (shunt) the door alarm, as user-configured, via a request to exit door motion sensor device or exit push-button. The capability shall be software programmable to allow selectable exit reporting.
- All system controlled electric locks shall be capable of being unlocked via a client workstation color monitor/keyboard and request-to-exit devices.
- The system shall provide for a completely downloaded and distributed database such that access control decision are made locally at the access controller and, in the event of the failure of the host computer or loss of communications to the host computer, the access control system shall continue to operate using full database information for all cardholders including security areas authorizations, time schedules, expiration dates of cards, holidays, etc. At no time after a card has been entered into the database of the file server and validated, shall the system fail to respond to an access request by a valid cardholder. (Restricted subsets of access control privileges and time schedule facilities in the distributed database will not be accepted).

**The access control system software shall, as a minimum, support the following features:**

- Cardholder records – 4,600 expandable up to 50,000 maximum

- Card readers - 256 Maximum
- Alarm input points – 1,024 maximum
- Relay outputs - 1,024 maximum
- Client workstations - 4 additional
- Operator passwords – 64
- 127 time schedules
- 16 user-defined alarm categories
- Local, hard and soft anti-pass back / anti-tailgate Configurable alarm-to-relay linking, downloaded to field controllers for local operation
- Configurable automatic time zone controlled commands, downloaded to the field controller for automatic local operation
- History/audit trail
- Alarm masking by operator
- Capability to define within the system variable card formats. q. Optional elevator control functions
- Optional capability to support multiple site and facility codes at card readers
- Optional capability to support biometric access control and verification readers (using smart card)

#### **DATABASE MANAGEMENT**

The system shall provide for the following Database Management capabilities:

- The software shall be capable of providing for the recall of system historical transactions with a minimum of 6,000 transactions recallable by operator command from the main event transaction file on the file server hard disk. Additional events may be recalled directly from an archived history log file on a removable hard disk cartridge.
- Data searching parameters shall be provided in the SACAM system software. The search capability shall include, but is not limited to the following:
  - Card Number, Serial Number, Employee Number or Name
  - Card readers
  - Security Areas
  - Alarm Points
  - Alarm Categories
  - Date and time periods
- The software shall provide report creation capabilities which offer search, organize and sorting according to the operator instructions, and have the ability to print, spool, or display a full report at a printer or client workstation.

- All operator commands and database entry functions shall be Internet Browser driven with plain English text and prompts, and the system shall provide on-screen ‘Help’ information by one click of a button. It shall also include multi-media help for certain critical functions.
- All access to the operator system functions shall require the entry of a valid password. A password must be used by the operator, manager, or administrator to access the system, with each password access authority being completely user-selectable by individual menu selection.

## 20. CCTV System

### General

- All systems and components shall have been thoroughly tested and proven in actual use.
- All systems and components shall be provided with a one-day turnaround repair express and 24-hour parts replacement. The manufacturer on warranty and non-warranty items shall guarantee the repair and parts expresses.
- Specifications included in this section are indicative and considered as a minimum; component and software that shall be acquired at the time of implementing the project shall be the latest versions available in the market.

### System Capabilities

- The system shall provide visual images from the cameras located through out the facility. The cameras located shall be fed into the Digital Video Server (DVS) located in the security room.
- The Main Security Control Room, which shall house the Monitors and the Digital Video Management Server.

### **HIGH RESOLUTION DOME CAMERA**

- The detailed specification of the camera is given below :

Pick Up Element	1/3" Interline Transfer Sony Super HAD CCD	
Signal system	PAL	NTSC
Pixel	795(H)x596(V) 542(H)x582(V) 811(H)x508(V) 542(H)x492(V)	
Scanning system	2:1 interline 625 lines	2:1 interline 525 lines
Sync. Mode	DC Internal	
Resolution	480 TVL	380TVL
Min. Illumination	0.4lux F1.6 (30 IRE,AGC ON)	
S/N Ratio	More than 48dB	
Auto iris mode	1/50 sec.	1/60 sec.
Auto iris lens type	DC Drive	
White Balance	ATW 2500K~9500K	
Focal length	3.5~8mm	
Iris range	F1.6~360	

Backlight compensation	Auto detect histogram plus 225 areas windows weight On /Off
Video output signal	BNC 1.0 Vp-p at 75 ohm load
Operating Temp.	-10C~+50C
Power source	DC12V
Power Consumption	3.5 W
Dimension	140x88mm

**DIGITAL VIDEO RECORDER**

- The Digital Video Recorder (DVR) shall be a Windows XP Embedded operating system with the functions of a recorder and multiplexer into one unit, having no tapes to maintain, replace or rewind.
- The embedded operating system shall result in increased stability and reliability and journaling file system allow for quick recovery in case of power interruptions.
- It shall have hardware and software watchdogs to monitor system operations. The DVR shall have manufacturer support on revision control on the hardware for 5 years from the date of manufacturing.

**System Architecture**

- The DVR can be placed on a shelf or desktop for easy access to the front panel control for operation with 4,8,16 camera configuration options.
- The recorder should include versatile multiplexer functions that allow live and recorded image from the 4 camera inputs to be shown on the monitor in a single camera, four camera, displays.
- It should also be possible to view live camera while recording.
- Shall have one VGA output for multiplexed viewing on GUI and one analog output for spot monitoring.

**Video Compression**

- The video compression should produce high resolution with play back. The System should have five user selectable image quality settings.
- The DVR should have a built in large volume 250 GB hard disk for both high reliability and high speed operation. Users should be able to select from 1 to 30 frames NTSC and 1 to 25 frames PAL by camera.
- The maximum recording frames per second shall be 480 frames NTSC & 400 frames PAL.

**Recording**

- Recording shall be user MPEG4 & the Time lapse recording adjustable by camera minimum of 1 frame every 10 seconds to maximum of 25 PAL or 30 NTSC. Recording speed shall increase automatically to maximum frame rates on event of alarms.



- System shall automatically proportion the available frame rates among cameras or user shall be able to assign different frame rates to each camera.
- The recording resolution of 320 x 240 or 640 x 480 NTSC and 352 x 288 or 704 x 576 PAL shall be available by camera. Recording shall also be triggered by motion detection with user definable sensitivity levels, and nine motion grids for each camera. Pre recording and post recording on event or alarm set by camera shall be available.
- Shall be provided with one channel audio recording and should be upgradeable to 16 audio inputs on request in the future.
- The compression shall be MPEG4 for storage and network transmission and shall have on-the-fly compression level adjustment on transmission.

#### **Play back**

- Shall be able Search recorded images single or multiple cameras.
- Shall have ability to search by date, time, or event. The alarm events shall be color coded by time for easy and quick access.
- On play back it shall have the ability to do digital zooming on the whole image or by selecting specific area on the screen.

#### **SMART SEARCH**

- Shall have SMART SEARCH facility, it should be motion based video detection and recording.

#### **Alarms**

- It shall have 8 inputs to trigger alarm recording with 4 outputs to drive external alarm devices. Alarms shall be activated manually or by event and associate any number of alarm devices with any cameras.
- Shall automatically without any operator intervention on event or alarm send out E-mail that attaches an image of the event or alarm in JPEG format.
- These Alarm Inputs shall be taken from the BMS system to activate instantaneous recording, depending on Fire Zones.
- All activities including system, sensor, motion and user activity shall be logged in the system automatically.
- It should be possible to record continuously or at a scheduled time periods. Search on recorded pictures shall be played back single or multiple cameras and shall have ability to search by date, time, event (alarm).
- All the alarm and events should be color coded by time for easy and quick search by the user.

#### **Video Export**

- The recorded images shall be exported in JPEG format with Digital watermark and also as AVI format for motion pictures.

- Shall have an inbuilt image authentication menu for picture verification. The storage medium shall be internal hard disk.
- The DVR shall have internal CDR for easy back up. Also the network capability shall allow the images are stored in the network devices which shall be done manually or pre defined schedule time periods to the ease of the user.
- During the back up the user shall be able to backup selected camera, date, and time as per requirement.

#### **Remote Monitoring**

- The DVR shall be provided with Remote Client software, which shall run on any TCP/IP network with Multiple DVR's addressable by IP addresses.
- Remote client shall be able to connect up to 32 DVR simultaneously and display the pictures. The DVR settings shall be locally and remotely configurable with user level name and passwords.
- It shall have facility to create Guest users with restriction to view only authorized cameras. The images shall be transmitted over the network in compressed format providing safe communication and reduction of load on the network.
- It shall have multiple password control levels – Settings, System Shutdown, Search, Network Access, Backup .
- It shall have administrator, user & guest level access to the system.
- The DVR shall be Web enabled so that it can be accessed to view live images by using an internet explorer by entering the IP, user name and password.
- The display screen with 16 segments shall have each segment for a specific DVR and shall display the selected camera on the window or switch between selected cameras within the same window in a sequence. Or from a single DVR it shall be able to display all the sixteen cameras on a single screen.
- From the central monitoring location the security officer shall be able to establish a two way voice communication to the specific DVR location through the same remote client software.
- The DVR shall be Web enabled to allow clients to access the DVR using standard Internet Explorer software for remote monitoring & control functions based on security parameters. Also the remote connectivity time out shall be programmable in minutes on the DVR to disconnect the users after a specified period of time after log in. This shall be used to prevent unnecessary traffic on the network.
- Note: Secure Internet Connection of sufficient Bandwidth, with Public Static IP shall be provided for by the Owner.
- The dimensions for the DVR shall be L x W x H in cm 53 x 42 x 17.5 for the Rack mount versions.

## 21. Building Management System (BMS)

The building management system shall be implemented for effective management, monitoring and Integration of various components like HVAC systems, Access Control systems, fire detection system etc.

The BMS shall perform the following general functions including but not limited to:

- Building Management & Control
  - Data Collection & archival
  - Alarm Event & Management
  - Trending
  - Reports & MIS Generation
  - Maintenance & Complaint Management
  - Network Integration
- The system offered shall be completely modular in structure and freely expandable at any stage.
  - Each level of the system shall operate independently of the next level up.
  - The system shall fully be consistent with the latest industry standards, shall be PC Based, operating on Windows 2000/XP or later, allowing the user to make full use of the features provided with these operating systems.
  - It shall combine the latest state-of-the-art technology with simple operating techniques and shall be used to control, manage alarms/reports and monitor the building service installations.
  - To provide maximum flexibility and to respond to changes in the building use, the system offered shall support the use of BACNET, LON, Modbus and Ethernet TCP/IP communication technologies.
  - The BMS shall be installed complying with all:
    - National and local statutory regulations,
    - Health & Safety at Work Acts,
    - IEEE Regulations
    - CE Conformity
    - Equipment manufacturer's instructions.
    - Regulations and conditions of BT, and utilities companies.

## 22. Water Leak Detection System

- The water leak detector shall be installed to detect any seepage of water into the critical area.
- It shall consist of water leak detection cable and an alarm module.
- The cable shall be installed in the ceiling & floor areas around the periphery.
- The Water leak detection cable shall be the sensor cable typically used to detect water leaks in the sub floor and above false ceiling areas.
- The Cable shall be capable of water detection over its entire length.
- The construction of the cable shall be of PVC Twisted pair, with SS 316 elements, of diameter not exceeding 3.5 mm.
- The Cable shall draw excitation signal from a start of the line module.
- This module shall serve as the interface between the Water leak detection panel and the Sensor Cable.
- The Start of Line Interface Module shall be locally placed in the False Flooring of the Server area(s), and shall be connected to the WLD Panel through standard 2 c x 1.5 mm<sup>2</sup> Cu- Ar Cable.
- The WLD Panel shall be capable of supplying power to the interface modules, and shall serve as the enunciator of alarms through facia mounted zonal LEDs.
- The panel shall activate sounders programmed Zone wise.
- Testing procedure shall involve physical application of a wet cloth to the cable, to test the relay operation.
- The Panel should sound the Alarms, and notify the BMS system.

## 23. Public Address System

The PA system is required for:

- Making public announcement from the Security Control Room and Facility Manager's room. Clear and crisp announcement should reach to the entire Facility area.
- Microphones should be provided to make announcements / respond to announcement from the designated location within the Facility.
- To play light music if required.

### 23.1. Common Alarm System

- The common alarm panel is required for checking the healthiness of all systems, to be installed at Data center.
- The panel can be installed in the room of Security Officer at Data center.

The common alarm panel should have provision for accepting "potential free" signals from all system for relevant status change in that system

## 24. Fire Proof Enclosures for Media Storage

Temperature to Withstand	1000° C for at least 1 hour
Internal Temperature	30° C after exposure to high temperature For 1 hour
Locking	2 IO-lever high security cylindrical / Electronic lock

### Compliance to Specifications

- All the hardware specifications mentioned in the RFP are the required minimum, higher or better specifications would be acceptable.
- Component furnished shall be complete in every respect with all mountings, fittings, fixtures and standard accessories normally provided with such component's and/or needed for erection, completion and safe operation of the component's as required by applicable codes though they may not have been specifically detailed in the technical specification, unless included in the list of exclusions.
- All similar standard components/parts of similar standard component's provided shall be interchangeable with one another.
- The methodology of cabling and installation work, to be adopted for the State Data Center, has to ensure minimum damage to the existing structure of the building. Any damage to the existing flooring/ walls/paint etc. shall be made good by the selected bidder.
- It is advised that bidder should visit site before submitting the tender to get apprised about the site conditions.
- The selected bidder shall be responsible for providing all materials, component's, and services, specified or otherwise, which are required to fulfill the intent of ensuring operability, maintainability, and reliability of the complete component covered under this specification within his quoted price.
- This work shall be in compliance with all applicable standards, statutory regulations and safety requirements in force of the date of award of this contract.
- The selected bidder shall also be responsible for deputing qualified personnel for installation, testing, commissioning and other services under his scope of work as per this specification. All required tools for completing the scope of work as per the specification is also the responsibility of the selected bidder.
- The selected bidder shall perform the services and carry out its obligations with all due diligence, efficiency, and economy, in accordance with generally accepted professional techniques and practices, and shall observe sound management practices, and employ appropriate advance technology and safe methods.

- The selected bidder shall always act, in respect of any matter relating to this contract or to the services, as faithful advisers to the Society for IT Initiatives Fund for eGovernance, Haryana
- The selected bidder shall furnish complete, well-fabricated and reliably operating and secure systems to Society for IT Initiatives Fund for eGovernance, Haryana .
- Design and selection of component and software shall be consistent with the requirements of long term trouble free operation with highest degree of reliability and maintainability.
- All components shall be constructed to operate safely without undue heating, vibration, wear, corrosion, electromagnetic interference or similar problems and all software shall be proven, tested and reliable.
- All interconnecting cables required to connect the communication component shall be furnished. All cables shall be fully assembled connector pre-terminated and factory tested as part of overall system checkout.
- Cables shall be neatly & properly tied up and dressed using appropriate cable hangers and Velcro bands. All the cables, connectors, sockets, panel's etc. shall be labeled for identification purpose.
- All the cabling should adhere to the TIA-942 Data Center Standard.
- All component, accessories and cables supplied under this contract shall be in accordance with the latest applicable recommendations, regulations and standards of:
  - CCITT/ITU
  - ANSI
  - IEC
  - IEEE
  - IETF
  - EIA/TIA 568 Standards
  - International Electro-technical Commission (IEC)
  - cable (Cat 6) and cable accessories (Cat6) UL Listed and verified
- For parameters not covered under the above codes, internationally acceptable standards shall be accepted.
- The selected bidder shall furnish a complete list of all standards and codes under which his component is designed, manufactured and assembled along with the bids.
- Functionality/accessibility of each component of the system and the system as a whole should be demonstrated to the satisfaction of Society for IT Initiatives Fund for eGovernance, Haryana.
- Reliable over voltage and over current protection circuits shall be provided in the component power supply units.

- The component power supply units shall be self protecting and also protect connected component's against interference, noise, voltage dips and surges & impulses that may be present in the mains power supply sources.
- Component shall be guaranteed for operation over the following AC power range to be made available by Society for IT Initiatives Fund for eGovernance, Haryana is 240 V AC +/- 10%, 50 Hz +/- 5%
- The Society for IT Initiatives Fund for eGovernance, Haryana shall provide suitable AC power at a single power point at one locations and distribution of this power to the various component's shall be responsibility of the selected bidder for which necessary distribution board, cable etc. shall be provided by the selected bidder.

## 25. Electrical Panels

### STRUCTURE :

- The Panels shall be of compartmentalized design so that circuit arc / flash products do not create secondary faults and be fabricated out of high quality CRCA sheet, suitable for indoor installation having dead front operated and floor mounting type.
- All CRCA sheet steel used in the construction of Panels shall be 2 mm. thick and shall be folded and braced as necessary to provide a rigid support for all components. Joints of any kind in sheet steel shall be seam welded, all welding slag grounded off and welding pits wiped smooth with plumber metal.
- The Panels shall be totally enclosed, completely dust and vermin proof and degree of protection being not less than IP : 54 to IS : 2147. Gaskets between all adjacent units and beneath all covers shall be provided to render the joints dust proof. All doors and covers shall be fully gasketed with foam rubber and /or rubber strips and shall be lockable.
- All panels and covers shall be properly fitted and secured with the frame and holds in the panel correctly positioned. Fixing screws shall enter into holes, tapped into an adequate thickness of metal or provided with bolts and nuts. Self-threading screws shall not be used in the construction of Panels.
- A base channel of 75 mm. x 50 mm. x 6 mm. thick shall be provided at the bottom.
- Panels shall be preferably arranged in multi-tier formation. The size of the Panels shall be designed in such a way that the internal space is sufficient for hot air movement. If necessary, openings shall be provided for natural ventilation, but the said openings shall be screened with fine weld mesh. All the electrical component shall be derated for 50°C.
- The Panels shall be provided with removable sheet steel plates at top and bottom to drill holes for cable / conduit entry at site.
- The Panels shall be designed to facilitate easy inspection, maintenance and repair.
- The Panels shall be sufficiently rigid to support the equipment without distortion under normal and under short circuit condition. They shall be suitably braced for short circuit duty.

### CIRCUIT COMPARTMENTS:

- Each MCCB shall be housed in separate compartments and shall be enclosed on all sides. Sheet steel hinged lockable door shall be duty interlocked with the unit in 'ON' and 'OFF' position.
- All instruments and indicating lamp shall be mounted on the compartment door. Sheet steel barriers shall be provided between the tiers in a vertical section.

### INSTRUMENT COMPARTMENTS:

- Separate adequate compartment shall be provided for accommodating instruments, indicating lamps, control contactors/ relays and control fuses etc.
- These components shall be accessible for testing and maintenance without any danger of accidental contact with live parts, bus bar and connections.

**BUSBARS:**

- The busbar shall be air insulated and made of high quality, high conductivity, high strength Aluminum.
- The busbar shall be of 3 phases and neutral system with separate neutral and earth bar. The size of neutral busbar in all main panels or lighting panels and feeders for panel shall be equal to phase busbar.
- The busbar and interconnection between busbars and various components shall be of high conductivity Aluminum.
- The busbar shall be of rectangular cross-section designed to withstand full load current for phase busbars and half rated current for neutral busbars in case of MCC panels only and shall be extensible on either side.
- The busbar size shall be as per the rating of the panel. The busbar shall have uniform cross-section throughout the length.
- The busbars and interconnections shall be insulated with epoxy-coated busbar. The busbar shall be supported on bus insulators of non flammable type with high creepage and high anti tracking property and non-hydroscopic SMC / DMC insulated supports at sufficiently close intervals to prevent busbars sag and shall effectively withstand electromagnetic stresses in the event of short circuit.
- The busbar shall be housed in a separate compartment. The busbar shall be isolated with 3-mm. thick bakelite sheet to avoid any accidental contact. The busbar shall be arranged such that minimum clearance between the busbar are maintained as below:

Between phases	:	25 mm. minimum
Between phases and neutral	:	25 mm.
Between phases and earth	:	25 mm.
Between neutral and earth	:	20 mm. minimum
- All busbar connections shall be done by drilling holes in busbars and connecting by chromium plated or tinned plated brass bolts and nuts.
- Additional cross-section of busbar shall be provided in all Panels to cover up the holes drilled in the busbar. Spring and flat washers shall be used for tightening the bolts.
- All connections between busbars and circuit breakers / switches and cable terminals shall be through aluminum strips of proper size to carry full rated current. These strips shall be insulated with insulating taps.

- Panel to panel entry of bus bar shall be effectively sealed by electrical and thermal insulation barriers so that products of flashover do not travel from one panel to another panel creating multiple faults.
- Busbar calculated on 50 deg. C. ambient temp. and 85 deg. C. for continuous and short time rating. Busbar surrounded air temp. shall be considered 70 deg. C. for busbar calculation
- All joint shall have non-flammable insulation shrouds for secondary insulation purpose

**ELECTRICAL POWER AND CONTROL WIRING CONNECTION:**

- Terminal for both incoming and outgoing cable connections shall be suitable for 1100 V grade, aluminum / copper conductor XLPE insulated and PVC sheathed, armored cable and shall be suitable for connections of solder less sockets for the cable size as per the feeder capacity.
- Power connections for incoming feeders of the main Panels shall be suitable for 1100 V grade aluminium conductor (XLPE) cables.
- Both control and power wiring shall be brought out in cable alley for ease of external connections, operation and maintenance.
- Both control and power terminals shall be properly shrouded.
- 10% spare terminals shall be provided on each terminal block. Sufficient terminals shall be provided on each terminal block, so that not more than one outgoing wire is connected to per terminal.
- Terminal strips for power and control shall preferably be separated from each other by suitable barriers of enclosures.
- Wiring inside the modules for power, control, protection and instruments etc. shall be done with use of 660 / 1100 V grade, FRLS insulated copper conductor cables conforming to IS . For current transformer circuits, 2.5 sq.mm. copper conductor wire shall be used.
- Other control wiring shall be done with 1.5 sq.mm. copper conductor wires.
- Wires for connections to the door shall be flexible. All conductors shall be crimped with solder less sockets at the ends before connections are made to the terminals.
- Control power supply to modules through the control transformer Control power wiring shall have control fuses, (HRC fuse type) for circuit protection. All indicating lamps shall be protected by HRC fuses.
- Particular care shall be taken to ensure that the layout of wiring is neat and orderly. Identification ferrules shall be filled to all the wire termination for ease of identification and to facilitate checking and testing.
- “CUPAL” washers shall be used for all copper and aluminum connections.
- Final wiring diagram of the Panels power and control circuit with ferrules numbers shall be submitted along with the Panels as one of the documents against the contracts.

**TERMINALS:**

- The outgoing terminals and neutral link shall be brought out to a cable alley suitably located and accessible from the panel front.
- The current transformers for instruments metering shall be mounted on the disconnecting type terminal blocks.
- No direct connection of incoming or outgoing cables to internal components of the distribution board is permitted; only one conductor may be connected in one terminal.

**WIREWAYS:**

- A horizontal / vertical metal / Al. wire way with screwed covers shall be provided at the top to take interconnecting control wiring between different vertical sections.

**CABLE COMPARTMENTS:**

- Cable compartments of minimum 300 mm size shall be provided in the Panels for easy termination of all incoming and outgoing cables entering from bottom or top.
- Adequate supports shall be provided in the cable compartments to support cables.
- All outgoing and incoming feeder terminals shall be brought out to terminals blocks in the cable compartment.

**EARTHING:**

- All earth bars of 50 mm x 10 mm shall be provided in the Panels for the entire length of the panel.
- The framework of the Panels shall be connected to this earth bar.
- Provisions shall be made for connection from this earth bar to the main earthing bar coming from the earth pit on both sides of the Panels.
- The earth continuity conductor of each incoming and outgoing feeder shall be connected to this earth bar.
- The armour shall be properly connected with earthing clamp, and the clamp shall be made for connection from this earth pit on both sides of the Panels.
- The earth continuity conductor of each incoming and outgoing feeder shall be connected to this earth bar.
- The armour shall be properly connected with earthing clamp, and the clamp shall be ultimately bonded with the earth bar.

**LABELS:**

- Engraved PVC labels shall be provided on all incoming and outgoing feeders.
- Single line circuit diagram showing the arrangements of circuit inside the distribution board shall be pasted on inside of the panel door and covered with transparent laminated plastic sheet.

**NAME PLATE:**

- A nameplate with the Panels designation in bold letters shall be fixed at top of the central panel.
- A separate nameplate giving feeder details shall be provided for each feeder module door.
- Inside the feeder compartments, the electrical components, equipments, accessories like switchgear, control gear, lamps, relays etc. shall suitably be identified by providing stickers.
- Engraved nameplates shall preferably be of 3 ply, (Red-White-Red or Black-White-Black) lamicol sheet. However, black engraved perplex sheet name plates shall also be acceptable. Engraving shall be done with square groove cutters.
- Nameplate shall be fastened by counter sund screws and not by adhesives.

**DANGER NOTICE PLATES:**

- The danger notice plate shall be affixed in a permanent manner on operating side of the Panels.
- The danger notice plate shall indicate danger notice both in Hindi and English and with a sign of skull and bones.
- The danger notice plates, in general, meet the requirements of local inspecting authorities.
- Overall dimensions of the danger notice plate shall be 200 mm. wide x 150 mm. high.
- The danger notice plate shall be made from minimum 1.6 mm. thick mild steel sheet and after due pre-treatment to the plate, the same shall be painted white with vitreous enamel paint on both front and rear surface of the plate.
- The letters, the figures, the conventional skull and bones etc. shall be positioned on plate as per recommendation of IS : 2551-1982.
- The said letters, the figures and the sign of skull and bones shall be painted in signal red colour as per IS : 5-1978.
- The danger plate shall have rounded corners. Location of fixing holes for the plate shall be decided to suit design of the Panels.
- The danger notice plate, if possible, it should be of ISI certification mark.

**INTERNAL COMPONENTS:**

- The Panels shall be equipped complete with all types of required number of Air circuit breakers, soft starters, switch fuse units, contactors, relays, fuses, meters, instruments, indicating lamps, push buttons, equipment, fittings, busbars, cable boxes, cable gland plates etc. and all the necessary internal connections / wiring as required.
- Components necessary for proper complete functioning of the Panels but not indicated in the BOQ 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 fully interchangeable.

**COMPONENTS:**

**GENERAL:**

- The type, size and rating of the components shall be as per the relevant feeder ratings.
- While selection of the capacity of the components resulting from the prevailing conditions like ambient temperature shall be allowed for.
- The thermal and magnetic trip rating shall be compensated for the ambient temperature.

**MOULDED CASE CIRCUIT BREAKER:**

- The moulded case circuit breaker (MCCB) shall be air break type and having quick make - quick break with trip free operating mechanism.
- Housing of the MCCB shall be of heat resistant and flame retardant insulating material.
- Operating handle of the MCCB shall be in front and clearly indicate ON/OFF/TRIP positions.
- The electrical contact of the circuit breaker shall be of high conducting non-deteriorating silver alloy contacts.
- The MCCB shall be provided microprocessor based overload and short circuit protection device.
- All the releases shall operate on common trip busbar so that in case of operation of any one of the releases in any of the three phases, it will cut off all the three phases and thereby single phasing of the system is avoided.
- The MCCB shall provide two sets of extra auxiliary contacts with connections for additional controls at future date.
- The electrical parameters of the MCCB shall be as per the description given.

**CONTACTORS:**

- The contactors shall meet with the requirements of IS : 2959 and BS : 7755.
- The contactors shall have minimum making and breaking capacity in accordance with utilization category AC3 and shall be suitable for minimum Class II intermittent duty.
- If the contactor forms part of a distribution board then a separate enclosure is not required, but the installation of the contactor shall be such that it is not possible to make an accidental contact with live parts.

**CURRENT TRANSFORMER:**

- Where ammeters are called for C.T.s shall be provided for current measuring. Each phase shall be provided with separate current transformer of accuracy Class I and suitable VA burden for operation of associated metering and controls.
- Current transformer shall be in accordance with IS: 2705 - 1964 as amended up to date.

**INDICATING LAMPS:**

- Indicating lamps assembly shall be screw type with built in resistor having non-fading colour lens. LED type lamps are required.
- Wiring for Remote ON, OFF, TRIP indicating lamp is required.
- Colour shade for the indicating lamps shall be as below :
  - ON indicating lamp : Red
  - OFF indicating lamp : Green
  - TRIP indicating lamp : Amber
  - PHASE indicating lamp : Red, Yellow, Blue
  - TRIP circuit healthy lamp : Milky

**Security**

The Solution implemented for SDC Project has to follow a well-defined security policy. It should provide a framework that ensures the availability, integrity, and confidentiality of information infrastructure.

The solution shall accomplish the laid objectives by providing identification, authentication, authorization/access control, administration and audit by incorporating a security architecture which is built upon a foundation of security services, relevant technologies, best practices, guidelines, and standards. The security services used to protect the information infrastructure shall include

- Identification – The process of distinguishing one user from all others
- Authentication – The process of verifying the identity of a user
- Authorization and Access Control – The means of establishing and enforcing user rights and privileges

- Administration – The process of establishing, managing, and maintaining security
- Audit – The process of monitoring the identification, authentication, authorization and access control, and administration to determine if proper security has been established and maintained.

It is important to note that the technologies chosen are in flux, where the services and goals remain constant. It is exigent that as new technologies emerge or existing one's mature that they be re-evaluated in light of the security principles and goals outlined in this document. These security services shall be delivered and that the technologies are implemented in conjunction with a set of best practices guidelines and industry standards.

Wherever applicable the following principles must be applied to the security architecture:

- All passwords must expire after a specified number of days or sooner at user's discretion.
- Reuse of passwords must be separated by a pre-determined number of alternate passwords, not to be less than 10
- User ID's not used within a specified period of time must be automatically locked out (length of lock out period to vary between existing and new user ID's)
- All the Systems should run most up-to-date anti-virus software to avoid malicious programs to cause damage to the systems
- The software solution must ensure that users create "strong" passwords.
- The application should allow Role Based Security Access to the application pages and features. The user should belong to a role based on functional role in the system and should have access only to execute the stated operations.
- The application should be configurable to provide role based security
- If a user ID enters an invalid password for more than 5 times the user id must be locked out and suspended until reset by an administrator. Also the system should not allow any malicious programs to execute at the server.
- The user profile variables like user id, session id, operational status has to be persisted in each client session and server should be able to track the user at any instance. Each access to the server has to be logged and should be based on digital certificates.
- The data transfer to and from the server should be secure to hacking and unauthorized access. The application should use a protocol to transfer the data with 128 bit encryption which could only be readable by the application deployed for the SDC Project.
- The User groups with appropriate roles have to be classified based on the privileges that are sought to be granted and users need to be assigned to the roles as appropriate. The supervisor has to be given appropriate privileges to assign people to roles. Access to all application modules and related functionality will be based on these privileges.
- Secondary authentication mechanisms like bio logon, smart card should be incorporated in the solution. These mechanisms should be used to for approvals of a process, executing high value transactions or to give access to sensitive information.
- Digital certificates for all servers, data encryption protocols to be supported (SSL).

- Assessing various touch points with external systems/networks and associated risks and risk mitigation measures should provided in the proposed solution
- All machines within the SDC Project Security boundary will participate in an IPSEC network, with machine certificates installed on identified hardware.
- All browser based access for the transactions performed from outside the integrated projects Security boundary must use Secure Socket Layer.
- All agencies external to the project will need to access the system via security firewall(s), except CSCs, which will have IPSEC enabled network.
- Information stored in the databases must be protected from unauthorized access.
- Any access to Database should only be via application authorization.
- Any administrative access to Database should only be via application authorization which should follow authentication of personnel by a suitable mechanism such as use of single-finger biometric technology.
- Backup/Restore: Backups should be secured against malicious use by unintended users.

Any activity that involves updation of database, such as generation of Bill Payment Receipt, should be done only by an authorized person. The logon information so obtained should be used to authorize and digitally sign the transaction using X.509 certificate/128 bit key that uniquely identifies the authenticated user. The document should be transmitted and stored in database as signed XML document. Hence a Bill Payment Receipt given to a citizen will have an equivalent digitally signed XML document stored in the secure database for non-repudiation.

The proposed Security architecture should provide creation and management of digital

- Certificates and PKI including:
- Capability to create and manage a Certification Authority.
- Issue and revoke certificates/keys and maintain appropriate trust lists.
- Use of digital certificates for 128-bit encryption and digital signatures.
- Location and Security Matrix

### **Compliance to ISO27001 Standards of Security**

- The technology solution should comply with ISO27001 standards and the DCO has to get the certificate of the same within three quarters” from the date of start of successful operations of the State Data Centre. Subsequently periodic surveillance audits must be carried out”. The cost incurred for obtaining and maintaining the certification shall be borne by the DCO.
- Security certification process shall include Audit of Network, Server and Application
- Security mechanisms.
- Assessment of authentication mechanism provided in the application /components /
- Modules Assessment of data encryption mechanism.
- Assessment of data access privileges, retention periods and archival mechanisms.
- Final output of this process would be a comprehensive audit report including all the Network, Server and Application security features incorporated in the project.
- Manageability Requirements of the project will be tested and certified for the following:

- Remote Monitoring of Status and Statistics of all high-level components
- Management capability to start/ stop/ restart services & systems.
- Auto discovery of all components manageable through SNMP
- Auto discovery of all other system components.
- Ability to track changes in configurations of the system components to help track
- Service/ System disruptions.
- Final output of this process would be a manageability compliance document for the system deployed.



## 26. Compliance to Specifications

- All the hardware specifications mentioned in the RFP are the required minimum, higher or better specifications would be acceptable.
- Component furnished shall be complete in every respect with all mountings, fittings, fixtures and standard accessories normally provided with such component's and/or needed for erection, completion and safe operation of the component's as required by applicable codes though they may not have been specifically detailed in the technical specification, unless included in the list of exclusions. All similar standard components/parts of similar standard components provided shall be inter-changeable with one another.
- The methodology of cabling and installation work to be adopted for the State Data Center has to ensure minimum damage to the existing structure of the building. Any damage to the existing flooring/ walls/paint etc. shall be made good by the selected bidder. It is advised that bidder should visit site before submitting the tender to get apprised about the site conditions.
- The selected bidder shall be responsible for providing all materials, components, and services, specified or otherwise, which are required to fulfill the intent of ensuring operability, maintainability, and reliability of the complete component covered under this specification within his quoted price. This work shall be in compliance with all applicable standards, statutory regulations and safety requirements in force of the date of award of this contract.
- The selected bidder shall also be responsible for deputing qualified personnel for installation, testing, commissioning and other services under his scope of work as per this specification. All required tools for completing the scope of work as per the specification is also the responsibility of the selected bidder.
- The selected bidder shall perform the services and carry out its obligations with all due diligence, efficiency and economy in accordance with generally accepted professional techniques and practices and shall observe sound management practices and employ appropriate advance technology and safe methods. The selected bidder shall always act in respect of any matter relating to this contract or to the services as faithful advisers to the Client.
- The selected bidder shall furnish complete, well-fabricated and reliably operating and secure systems to Client. Design and selection of component and software shall be consistent with the requirements of long term trouble free operation with highest degree of reliability and maintainability. All components shall be constructed to operate safely without undue heating, vibration, wear, corrosion, electromagnetic interference or similar problems and all software shall be proven, tested and reliable.
- All interconnecting cables required to connect the communication component shall be furnished. All cables shall be fully assembled connector pre-terminated and factory tested as part of overall system checkout. Cables shall be neatly & properly tied up and

dressed using appropriate cable hangers and Velcro bands. All the cables, connectors, sockets, panel's etc. shall be labeled for identification purpose.

- All the cabling should adhere to the TIA-942 Data Center Standard.
- All component, accessories and cables supplied under this contract shall be in accordance with the latest applicable recommendations, regulations and standards of:
  - CCITT/ITU
  - ANSI
  - IEC
  - IEEE
  - IETF
  - EIA/TIA 568 Standards
  - International Electro-technical Commission (IEC)
  - cable (Cat 6) and cable accessories (Cat6) UL Listed and verified
- For parameters not covered under the above codes, internationally acceptable standards shall be accepted. The selected bidder shall furnish a complete list of all standards and codes under which his component is designed, manufactured and assembled along with the bids.
- Functionality/accessibility of each component of the system and the system as a whole should be demonstrated to the satisfaction of Client.
- Reliable over voltage and over current protection circuits shall be provided in the component power supply units. The component power supply units shall be self protecting and also protect connected component's against interference, noise, voltage dips and surges & impulses that may be present in the mains power supply sources. Component shall be guaranteed for operation over the following AC power range to be made available by Client: 240 V AC +/-10%, 50 Hz +/- 5%
- The Client shall provide suitable AC power at a single power point at one locations and distribution of this power to the various component's shall be responsibility of the selected bidder for which necessary distribution board, cable etc. shall be provided by the selected bidder.

## 27. Glossary of Abbreviations

IT	Information Technology
SDC	State Data Centre
LAN	Local Area Network
HIPS	Host Based Intrusion Prevention System
SAN	Storage Area Network
VLS	Virtual Library System
EMS	Enterprise Management System
KVM	Keyboard, Video Display Unit and Mouse Unit
UPS	Uninterrupted Power supply
NOC	Network Operating Center
PVC	Polyvinly Chloride
CCTV	Closed Circuit Television
BMS	Building Management System
SWAN	State Wide Area Network
CSC	Common Service Center
DCO	Data Center Operator
MBPS	Mega Bytes per second
GBPS	Gigabits per second
IEEE	Institute of Electrical and Electronics Engineers
VLAN	Virtual Local Area Network
IGMP	Internet Group Management protocol
IP	Internet protocol
OSPF	Open Shortest Path First
RIP	Routing Internet Protocol
HSRP	Hot Standby Router Protocol
VRRP	Virtual Router Redundancy Protocol
ACL	Access Control List
FTP	File Transfer Protocol
TFTP	Trivial File Transport Protocol
SNMP	Simple Network Management Protocol
CLI	command line interface
GUI	Graphical User Interface
DMZ	demilitarized zone
GBIC	gigabit interface converter
SFP	Small form-factor pluggable
LACP	Link Aggregation Control Protocol
MAC	Media Access Control
QoS	Quality of Service
NTP	Network Time Protocol
VPN	Virtual Private Network
NAT	Network Address Translation
PAT	Port Address Translation
PPP	Public Private Partnership
HDLC	High-Level Data Link Control
MPLS	Multi-Protocol Label Switching
PIM-SM	Protocol Independent Multicast - Sparse-Mode
PIM-DM	Protocol Independent Multicast - Dense-Mode
MOSPF	Multicast Open Shortest Path First
SSH	Secure Shell
ARP	Address Resolution Protocol
P2P	Point to Point

XML	Markup language for documents containing structured information
ICMP	Internet Control Message Protocol
UDP	User Datagram Protocol
SMTP	Standard Mail Transfer Protocol
HTTP	Hypertext Transfer Protocol
SNMP	Simple Network Management Protocol
DNS	Domain Name System
NetBios	Network Basic Input/Output System
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
DES	Data Encryption Standard
AES	Advanced Encryption Standard
RTP	Real-Time Transport Protocol
PPPoE	Point-to-Point Protocol over Ethernet
DHCP	Dynamic Host Configuration Protocol
URL	Uniform Resource Locator
TACACS	Terminal Access Controller Access-Control System
AAA	Authentication, Authorization and Accounting
SLA	Service Level Agreement
DBA	Data Base Administrator
JVM	Java Virtual Machine
MTTR	Mean Time to Repair
MTBF	Mean Time between Failure
STOP	Stack Overflow Protection
RR	Resource Record
DLT	Digital Linear Tapes
SMF	Sealed Maintenance Free
MCCB	moulded case circuit breaker
LBS	Load bus synchronization system
PDU	Power Distributions Units
ATS	Automatic power transfer switches
STS	Static Transfer Switch
AVR	Automatic Voltage Regulator
UL94 V-1	Underwriters Laboratory Specification 94 with V-1 rating
RCC	reinforced cement concrete
MCP	Manual call points
AHU	Air Handling Units
TXV	Thermostatic expansion valve
HSSD	High Sensitivity Smoke Detection System
NEC	National Electrical Code