Guidelines

For

Technical and Financial Support

For

Establishment of State Data Centre (SDC)

Department of Information Technology,
Govt. of India, Electronics Niketan,
New Delhi – 110 003.

1.0 Preamble

1.1 State Data Centre (SDC) has been identified as one of the important element of the core infrastructure for supporting e-Governance initiatives of NeGP. Under NeGP, it is proposed to create State Data Centres for the States to consolidate services, applications and infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services. These services can be rendered by the States through common delivery platform seamlessly supported by core Connectivity Infrastructure such as State Wide Area Network (SWAN) and Common Service Centre (CSC) connectivity extended up to village level. State Data Centre would provide many functionalities and some of the key functionalities are Central Repository of the State, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration.

2.0 Background

2.1 The State Data Centre is a key-supporting element of e-Government Initiatives & businesses for delivering services to the citizens with greater reliability, availability and serviceability. SDC provides better operations & management control and minimizes overall cost of Data Management, IT Management, Deployment and other costs.

2.2 State Data Centre acts as a mediator and convergence point between open unsecured public domain and sensitive government environment. It enables various State departments to host their services/applications on a common infrastructure leading to ease of integration and efficient management, ensuring that computing resources and the support connectivity infrastructure (SWAN/NICNET) is adequately and optimally used.

2.3 The design of Data Centre represents many challenges and is a complex task as it involves many stakeholders (state departments having varying

requirements, access mechanism and delivery channels to the citizens). The extent to which the SDC must remain operational even when some of its resources are impaired or unavailable will greatly influence how the design objectives of Reliability, Availability, Scalability, Serviceability and also Backup, Redundancy, Survivability and Disaster Management are met.

The SDC will be equipped to host / co-locate systems (e.g. Web Servers, Application Servers, Database Servers, SAN, and NAS etc.) to host applications at the SDC to use the centralized computing power. The centralized computers/Servers will be used to host multiple applications. SDC will have high availability, centralized authenticating system to authenticate the users to access their respective systems depending on the authentication matrix.

2.4 Department of Information Technology (DIT) has taken note of the broad requirements for a typical data centre which include infrastructure facilities (physical, electrical, air conditioning etc.,) installation and integration of IT infrastructure (servers, telecom equipment, integrated portal/ departmental information system, Enterprise and network management system, security, firewalls/IDS, networking components etc.), software and databases. Establishing a State Data Centre is a complex task and requires substantial investment and efficient Operations and Management. Therefore it may be prudent to utilize the services of existing IDC players in the country with due and adequate security and policy measures/considerations. The paramount consideration in any arrangement is the security of the data and the preservation of the ownership and control of government data, both de jure and de facto.

3.0 In view of the above, DIT has formulated the Guidelines to provide Technical and Financial assistance to the States for setting up State Data Centre. These Guidelines also include the norms for outsourcing of the SDC to a private/ public sector service provider including some of the technical and administrative

norms to be followed by the States, depending on the implementation option adopted by the State to establish the SDC.

3.1 While formulating the Guidelines, DIT has noted that some State Governments would have different approach to State Data Centre while hosting applications at the SDC. In case States are using repository of Servers at the District level, the SDC in such case may act as a central repository for consolidation of the disaggregated resources.

3.2 Department of IT has also taken note of the proliferation/size of applications to be hosted at the SDC and has built-in provisions to ensure future scalability of the SDC while determining its initial sizing.

3.3 For the purpose of the sizing of the State Data Centre, the States have been put in three categories of Large, Medium and Small based on the population/ number of districts in each State.

4.0 Implementation Options

4.1 State would need to establish the SDC using any one of the two options indicated below:

Option I: State/UT and NIC together form a composite team for the State Data Centre. While sovereign control of the data/ applications shall be with the State (both de- jure and de-facto); NIC through its dedicated core team (6-7 domain experts /professionals) which may be specially created for each State, shall provide complete handholding for infrastructure up-keep, operations & management including issues related to business continuity. NIC Data Centre team would further be supported by domain specialists and support staff that would to be recruited by the Centre/State for the State Data Centre. The Facility Management services for physical infrastructure may be outsourced, if required.

However, for this option a tightly coupled administrative and techno-functional arrangement with clear roles and responsibilities of both the State IT department and State NIC Data Centre team shall be put in place and implemented. The Data Centre administrative responsibility shall be with State IT Secretary, the technical and day to day operations shall be the responsibility of the designated NIC Data Centre Project Manager. While the Project Manager shall functionally report to State IT Secretary; for all matters related to State NIC team, he/she shall report to DG NIC.

In case of any issues involving higher level intervention, an Apex Committee chaired by the Chief Secretary of the State with DG-NIC as co-chairman is suggested. Other members of the committee shall be State IT secretary, NIC Project Manager and a representative from DIT.

Template RFP for this option shall be made available to the States including a consulting agency by DIT. The consultancy agency would assist the States for project development (DPR), bid process management, supervision and overall implementation of the State Data Centre.

Option II : The State/UT leverages the capabilities of existing commercial Internet Data Centres (IDCs) for which different deployment models are available i.e. Co-located services, Dedicated Services and Managed Services. Under this option, the State may identify a suitable model (confined to either co-located services or dedicated services only keeping in view the security implications) to select an appropriate agency through a suitable competitive process for outsourcing. The entire process of outsourcing, including advising on the most appropriate model, would be managed by the consulting agency to be made available by DIT to the State. Template RFP for this option shall be made available to the States by DIT. Depending upon whatever outsourced model is selected by the State, Servers will be owned and operated by State and the management of the Data/Information shall be under the direct control of the State both de-jure and de-facto. For this, the State would require to deploy a dedicated

team which includes Project Manager (equivalent to Data Centre Manager), DBA, System administrator, Network Administrator, Support Staff etc as broadly indicated at Annexure 4 of the policy guidelines. Further, the State may also exercise the option to engage and utilize the manpower resources of NIC. States would not be permitted to choose implementation Option- II unless one of the following two criteria is met:

i. The Core Data Centre team is headed by a Project Manager drawn from the NIC. For this arrangement a mutual agreement between the State Government and NIC shall be worked out.

OR

ii. The State Government would have to satisfy the DIT/Empowered Committee set up by DIT, regarding their technical competence and ability to handle the security issues involved adequately, while hosting their Data/Applications in a commercial IDC.

For both Option I & II, the State would need to designate an appropriate Central/ State agency to take overall responsibility for receipt of funding support, implementation and rendering accounts/ Utilization Certificates.

Whatever options as above that may be exercised by the States, necessary Service Level Agreement would be defined and SLAs finalized. An implementation committee shall be constituted by the State with a representative from DIT and State NIC as members of the committee.

4.2 Depending upon whatever option as above is adopted by the State, the essential requirements as regards physical security, access mechanism, data protection and security, confidentiality, privacy issues and business continuity plan would need to be complied with, by the State in view of the sovereignty /sensitivity of the databases and the applications hosted in the SDC. These have been attached at Annexure -1 & 2 to the Guidelines to

help/guide the State. Further, the stipulations/standards on data security, computing environment and storage environment have also been elaborated at Annexure -3 for the benefit of the State.

5.0 Eligibility Conditions for States for DIT funding support.

5.1 States should have initiated action for setting up of SWAN, which shall provide connectivity between the proposed Data Centre site, and the Secretariat ,various Departments and at District and Block level, wherever, required.

5.2 The State would need to have undertaken implementation of at least three major statewide e-governance projects/services/applications that require creation of SDC of which at least one should have been completed in order to be eligible for funding support.

6.0 Norms for Sharing of Cost between GoI and State Govts.

6.1 GoI support will cover the entire cost of establishment, operation and maintenance of the State Data Centre for a period of five years on 100% grant-in-aid basis. The financial assistance being provided to the States shall include refurbishing of the physical space to the Data Centre requirements including back-up power supply (UPS and DG sets) and Air-Conditioning requirements. The cost of consultancy for option I and consultancy for undertaking technical feasibility study, advising on most appropriate model, preparation of SLA, etc. in case of Option II, will be provided as 100% grant by DIT to the agency designated by the State to undertake the selection of the IDC service provider. The cost of monitoring of performance under SLAs would also be covered by GoI support, including cost of engaging a third party for such monitoring/audit of the SDC.

6.2 The cost of manpower required for domain specialist team for Data Centre operations & management over a period of 5 years shall be provided by the GoI.

6.3 For planning purposes, the sizing of the Data Centre has been classified in three categories: Large, Medium and Small which shall also depend upon the number of applications and the data size. Accordingly, the funding to the States may vary with adequate provision built-in, for upgradation/scaling of the Data Centre during the initial period of 5 years.

7.0 Exclusions from DIT funding support

7.1 The physical space required for the Data Centre would be the responsibility of the State. A well secured area for the SDC would be demarcated. The demarcated area should have readily available power connection preferably from two different sources, water connection and other civic amenities.

7.2 The Back-End computerization of the Deptts would be the responsibility of the State and no financial support is envisaged in this regard as part of State Data Centre.

7.3 The cost of providing connectivity to the State Data Centre would be outside the scope of the Data Centre. The State can connect the Data Centre to the State PoPs, which is being provided by the DIT as part of SWAN scheme.

7.4 The cost of providing connectivity to the Disaster Recovery from the Primary Data Centre Site and the Internet bandwidth required at the Primary & DR site would be outside the scope of the Data Centre Scheme and shall be borne by the State.

7.5 Any incremental investment beyond 5 years period would be the responsibility of the State.

8.0 Deployment Architecture for delivery mechanism

8.1 The architecture of a Data Centre would be such as to provide a model environment capable of handling the typical business model of dynamic change supporting multiple G2G, G2C, G2B, B2C activities across all channels like CSCs, portals, kiosks etc. As e-Governance applications are expected to grow, the Data Centre architecture shall be highly scalable and be built on a solid architectural foundation. The power and cooling system should at least meet with Tier-I requirements with possibility of upgrading to the next level. The State Data Centre Architecture would be multi-layered architecture and the applications to be hosted in the Data Centre shall support interoperability standards like XML, SOAP etc. The State Data Centre would provide infrastructure such as firewall service, directory service, web service, database service, portal, integration, management, data storage services and possibly a standards based messaging Gateway, which could be a shared infrastructure to all the applications / departments in the State Data Centre.

9.0 Data Centre Management and Monitoring

9.1 A centralized management and monitoring system (tool) capable of doing fault management, configuration management, security management, report generation, alerting, monitoring the critical servers, log monitoring and Data Centre network and security infrastructure etc. would be part of the Data Centre. This system/tool would be scalable as well as be able to provide a hierarchical troubleshooting. In case, the Enterprise Management and Monitoring tool is already available for SWAN, the same would be utilized for State Data Centre requirements as well.

10.0 Service Availability & its Monitoring

10.1 End-to-end service availability of the SDC and its independent monitoring is the prime requirement to have reliable, seamless, smooth delivery of the services

to the citizens and other G2G & G2B applications meeting the objectives of this core e-Governance infrastructure. It is, therefore, necessary that appropriate Service Level Agreements (SLAs) be worked out between the States and the Implementing Agency and that an Independent Agency would be appointed to monitor the performance with reference to the SLA and related aspects.

11.0 Disaster Recovery and Business Continuity Plan

11.1 The high availability is one of the critical requirements of the Data Centre. As the systems are centralized at Data Centre, the State would be required to establish appropriate Disaster Recovery and Business Continuity Plan (DR and BCP) along with appropriate data backup and recovery infrastructure. Initially, State should plan for off-site Back-up mechanism for their DR strategy and depending upon mission critical requirement the BCP requirement would be met through the design architecture of the primary Data Centre itself.

The Disaster Recovery (DR) arrangement has been envisaged to be established and provided by NIC. NIC is in the process of setting up National Data Centres at Hyderabad and Pune of the order of 8000 sq. ft. each, apart from existing National Data Centre at Delhi. These centres will be connected through high speed networks to support data/application back-up facility and likely to be operational within one year time frame. While these centres will house largely central government data, these would have enough capacity to be used as DRs for the SDCs on a regional basis. One more Data Centre to take care of the Eastern region is planned to be setup by NIC at Bhubaneswar for which a budget provision over 5 years period has been included in the SDC scheme outlay.

12.0 Data Retention Plan

12.1 The State would formulate an appropriate Data Retention policy and ensure that the data centre architecture supports the same. The Data Retention Policy would be guided by the following factors:

a. Data classification and risk assessment of data.

b. Data Retention Period.

c. Data Security aspects.

d. Disposal of data once the retention period is over.

13.0 Data Centre Protection

13.1 The data centre shall have the required protection and safeguard mechanism for physical security, network security and facility infrastructure requirements including protection against fire, natural calamity and man made risks.

14.0 Security Audit

14.1 The State shall get the security audited by third party expert periodically (once in six months) and as and when there is significant upgradation of systems which include hardware, software and network resources to ensure and guarantee security of the Data Centre. The audit shall bring out any security lapses in the system and establish that the system is working as desired by the State.

15.0 Management and Administrative Control

15.1 Whatever options the State may opt, the overall management control shall be with the State Government both de jure and de facto. The State will be responsible for compliance with all guidelines through its designated Department/Agency. However, appropriate agreements to give effect to this, may be worked out between the State and the outsourced vendor wherever required.

Annexure – 1

Best practices and Guidelines to Physical Security of the State Data Centre

The Data Centre should ideally be built in a central location within the building complex. An approximate area of 4000 sq. ft. would be required for the Data Centre. The flooring should be capable of handling full load of the equipments hosted at the Data Centre. An ideal location for the Data Centre would be the first floor. It should never be built in the basement or at the top floor. It would be difficult to maintain the environmental & physical controls at the basement or at the top floor. Lifting of heavy servers, SAN boxes, UPS, etc. to the top floor will also be difficult. The proposed Data Centre space /floor should be free from water leakages from the floors which are above and below it.

The Data Centre area should be logically divided in Zones based on the level of security as described below:

Zone A: is the DC Server room area that has server racks, storage racks and networking equipment. The area required for Zone A should approximately be 1500 sq. feet.

Zone B: comprises of NOC room, reception area, Help Desk area, Call Centre, Testing/Monitoring room. This zone requires approximately 1500 sq. feet.

Zone C: comprises of room for power panels, BMS Manager Room, AHU, UPS, Telecom Room, etc. This zone requires approximately 1000 sq. ft.

The rack should be designed taking into consideration the maximum amount of cooling for equipments / servers. Modeling techniques such as Thermal modeling should be used to arrive at the placement of racks in the DC server room.

1.0 Design Parameters

1.0 Data Centre Floor Usage Allocation

The facilities could be divided into the following sections according to usage and reliability requirements:

ZONE A	ZONE B	ZONE C
Server racks, Networking racks, Structured cabling racks, Storage Area Network box, High end Servers, etc	• NOC Room (Network Operation Centre) • Centralized Building Management Systems (BMS) monitoring room • Help-Desk Area • Testing / Lab Room	• Electrical Room (Power Supply room) • Telecom Room • UPS and battery room • AHU • Fire Suppression System

1.1 Air conditioning

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

Zone A: ***Zone A should be provided with precision air conditioning on a 24 x 7 operating basis at least meeting with Tier – I 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. The units should be down-flow fashion, air-cooled conditioning system.***

Zone B/C: ***Zone B/C should be provided with split-type comfort air-cooled system (at least meeting with Tier – I 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.

General Description of Equipment

The equipment should be manufactured to ISO 9001 quality assurance standard and should be factory tested prior to dispatch. These units should be factory assembled which confirms to the following.

- Air Filtration conforming to EU3 standards with 50mm thick disposable pleated cell filters fitted on the return airside of the evaporator coil and having a maximum efficiency of 30%.

- Cabinet conforming to Class 1 BS 476 Part 6 & 7 standards.

- Electric Re-heater should be operating at black heat temperature and should be protected against airflow failure and overheat cutout.

- Humidifier should be capable of having an adjustable capacity control ranging from 40%-100%. The steam cylinder should be constructed from high temperature and should be suitable for operation on mains water without use of a break tank. The humidifier should be equipped with an automatic water supply and flushing system.

- Power Panel should be capable of operating at 420V, 3 phases, and 50Hz electrical supply and should be capable of withstanding voltage variation of ±5%. A main isolator should be provided and sized accordingly to meet the systems total power requirements. Within the panel individual power loads should be distributed equally across the three phases and all individual wires should be color-coded and numbered to facilitate ease of servicing.

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 server room should have an emergency panic latch door with automatic alarm system. The vendor should provide a fireproof cabinet to store on-site backup tapes taken daily, weekly, monthly and half-yearly. Walls for the Data Centre should be Fire-Rated to prevent any further spread of fire.

1.2 Microprocessor controller Panel

The control panel makes it easy for the user to have all the data and factors available in a precise, clear, and easy to understand manner at all times. The display panel should be located on the front of the unit with LCD display for monitoring and alarm indication of the followings.

- Status indication
- Cooling on
- Electric heating on
- Humidifier on
- Dehumidifier on
- Alarm Indication with Visual & Audible
- Power failure
- Fan overload
- Humidifier power fault
- Humidifier control fault
- Heater fault
- Airflow failure
- Change filter
- Control circuit trip
- Return air temperature / RH out of range
- Supply air temperature out of range
- Return air humidity sensor alarm
- Return air temp. Sensor alarm

- Data Error
- Service alarm
- Electric heater alarm
- Microprocessor fault
- Humidifier flood
- Water leakage alarm
- Smoke alarm

The Control panel should provide comprehensive alarms & status indications, having the following functions: -

- Graphical display of temperature and humidity curves over the last 24-hour.
- Self-diagnostic functionality.
- Supply air fan surge to let fan continue on operation for a period of 180 second before total shutdown.
- An automatic changeover for duty / standby unit's base on time interval setting and any failure of duty unit.
- An automatic restart function with sequence start program to prevent power surge during start-up on multi-system installation.
- A graphic display to review the return air temperature and humidity condition.
- Comprehensive event storage system by date and time of occurrence.
- Should be capable of connecting to tele-monitoring systems and other building management systems by means of an open interface.
- Simple user-friendly operating guidance.

1.3 Electrical System

1.3.1 Availability for distribution system:

The distribution system should meet with tier – I requirements and should have enough provision to scale up if required in a later stage. It should have provision for Dual Bus configuration in order to have dual power supplies to each rack, thus minimizing downtime during maintenance operations. Dual feeders

should also be provided for incoming feed from the main feeder.

1.3.2 Redundancy:

Power Supply for each rack should be from different power sources. The concept is based on n + 1 redundancy, where n is the number of systems or main items of equipment required to maintain the specified operational requirements. That means, failure of a single such system or equipment item can be tolerated.

1.3.3 Switchboard

All switchboards should be designed to support non-linear load with neutral conductors at least 1.7 times or 2x phase/line conductors, this is as per IEEE1100-1999 specifications. Panel boards should be divided into two, one from UPS and the other from generator. These panels should be installed separately in their respective zones.

Incoming electrical lines should have primary and secondary Transient Voltage Surge Suppressors (TVSS) installed, primary TVSS just after the Main LT switchboard and secondary just before the UPS. The primary should take care of very high transients (kilovolt range) caused by lightning strikes or HT surges and the secondary should take care of what ever manages to pass through (several hundred volts in range) the primary TVSS.

1.3.4 Lighting:

Adequate illumination (Lux) should be designed for the Data Centre. The illumination can be divided into two zones; specific rooms & other areas. Power source for lighting in these specific rooms should be from Emergency Panel for high availability purpose.

10% of the power for lighting in other areas should be from emergency panel and the rest from direct electricity board. Emergency panel should supply

lighting on Walkway and emergency exit path.

Lighting on rack area and cage area need to be adjusted in order to eliminate lighting in un-proper areas such as over the top of the rack for the purpose of energy saving and cost saving.

1.3.5 Grounding:

Design of grounding should be a single ground system with separated ground window for power and data conforming to international standards.

1.3.6 UPS System:

UPS System design concept is based on redundancy and availability, with 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 another UPS system. Dual redundant UPS systems will take care of following needs -

- Computers within the Data Center
- NOC equipment/ Workstations
- Emergency Lighting
- 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.

1.3.7 Generator

The Data Centre should have generator set to take care of high availability. The generator should have adequate capacity to supply to full load specifications.

1.3.8 Surge Protection System

Surge protection should be installed at switchboard to suppress surge and EMI conforming to IEEE62.41 and UL1283.

1.3.9 AMF Panel

The Data Centre should have an AMF Panel connecting the DG, UPS such that automatic switchover takes place during power failure.

1.4 Surveillance

1.4.1 Video Surveillance

Video Surveillance or CCTV System has to be provided mainly for security purposes. Adequate units of cameras should be installed to cover all areas of the Data Centre and premise surveillance. All these cameras should be coupled with motion sensors so that cameras can start recording only when they detect movement in the corresponding area. All the data should be recorded in digital format onto hard disk/Tapes for future investigation. There should be a central monitoring room to monitor the movement in the Data Centre & premises.

1.4.2 Access Control

Proximity card reader and proximity access control system should be installed with its software for monitoring the access of individual persons in the Data Centre. This should be installed inside as well as outside the Level 2 premises.

Biometric authentication should be deployed at the main access door of the server room area (Level 3). This device should support fingerprint scanning and numeric authentication.

1.5 Civil Work Specification

1.5.1 Raised floor and insulation

Cement fill raised floor panel with anti-static finish should be installed on bolted-stringer system in order to maintain more rigidness and stability for the concentrate load and rolling load. This type of system is better for frequent panel movement.

Insulation under the raised floor should be provided to prevent the condensation caused by down-flow conditioning within DC area and network area. Perforate panels should be provided for at least 10% of total DC area and network area.

Galvanized coating for materials such as ceiling grids, raised floor supports, etc should be electroplated galvanized. This is to avoid zinc whiskers or metallic contamination.

1.5.2 Water Leak Detection System

Sensing cable should be installed along room perimeter especially along the glass windows, and wall area, toilet adjacency area, and under air condition units in order to sense liquid leakage.

1.5.3 Fire Detection

Industry standard ionization and photoelectric detectors should be installed all over the Data Center area. A separate fire alarm panel should be deployed for Data Centre area. In case of fire detection, this panel should communicate the alarm signal to the master fire panel that monitors the entire premise. It should also have the capability to send audio/visual signal at security area.

The whole system should have fire detection and alarm panels along with manual

call stations. For added protection, Very Early Smoke Detection System (VESDA) should be installed for the server room area only. The technology is based on lasers and very effective for detecting fire possibilities.

1.5.4 Fire Suppression

The entire Data Centre is divided into two major areas, critical and non-critical. The critical area consists of server room (Zone A) and non-critical areas consist of other areas (Zone B, C).

NFPA standard 2001 compliant fire suppression system should be installed for Zone A. For other areas, hand-held fire fighting devices should be installed at accessible locations; these are primarily CO2 gas based Fire Extinguishers.

1.5.5 Pest Control & Rodent Repellent & System

Pest Control system should be provided for the entire Data Centre & Rodent repellant system should be provided mainly in areas where false flooring is provided within the Data Centre. The electronic Repellent system shall be provided in such a manner so as to protect the entire volume of space under consideration including above false ceiling, below false ceiling and below false floor.

1.5.6 Architectural Work

Architectural design of the Data Centre should be done considering the following key parameters areas:

- Space Planning
- Lighting
- Redundancy factors
- Color Scheme

Idea of area zoning for the architecture is based on the security purpose and practical situation. Customer accessible area should be near to the reception counter, an existing area. This is the first cut off area for visitors. NOC room and monitoring rooms should be located just after the reception and should have proximity card security. Ease of accessibility and scalability should be taken into consideration for designing the rooms. Permanent lighting fixtures should be installed to give lighting intensity of approximately 350-400 Lux.

A separate entrance is recommended for access to UPS/Power room, and client room maintenance. The technician and engineers will frequent these areas.

Access to Data Centre can be from main entrance near NOC room, and from monitoring room. For bringing in racks and systems, a dual door of at least 6ft wide should be provided. In normal operation this door should be closed and locked. Access control mechanism would not be required for this door or this door can be used as emergency exit and emergency door opening system.

1.5.7 Monitoring System

The monitoring system for all the installed equipments should be installed in one centralized panel at NOC room, which can monitor the following equipment(s):

- Water leak Detection
- On and Off of Air-conditioning system, and its alarm
- Humidity and Temperature

All the systems proposed should be connected to a BMS system. Planning for the BMS should accordingly be carried out.

Annexure - 2

Best practices and Guidelines to the States on Data Security, Privacy, Confidentiality and Protection

I) Accessing Data but staying in control of data security

The State would follow the best practices in Data Security while sharing the Data from the SDC. To ensure that security is implemented and maintained within the State Data Center, a security policy would be developed and enforced. The security policy must include the following:

- The overall security goals.
- An outline of the overall level of security required.
- The security standards, including auditing and monitoring strategies.
- Definitions of training and processes to maintain security.

State would deploy Defense-in-depth strategy for securing the State Data Center architecture and enhance security level. This would comprise of Perimeter Defenses, Network Defenses, Host Defenses, Application Defenses and Data &Resources Defenses.

1. State would formulate and implement Trust and Identity Management Policy. This is done to permit only authorized users and administrators to access data center resources.

- Authenticate users prior to accessing services from the SDC, which would provide accountability for the transactions/activities performed within the system.

- State would use Public Key/Private Key infrastructure for AAA access mechanism to the users for providing access to the sensitive transactions.

- State departments would need do risk assessment of the services/transactions processed using the information systems. For the critical and sensitive online transaction (e.g. e-procurement tender response), PKI based authentication shall be used.

- State would use digital Signature, Digital certificates/biometrics for authentication of users performing critical transactions in the system (e.g. for performing tax changes to the tax related values (master tables in the system, PKI/biometrics based authentication is required).

- In case of less sensitive data, State would use token based or strong password based authentication mechanism for services/transactions where public key certificates are not feasible.

2. State would do a security posture assessment to identify vulnerabilities and risks, with specific breakdown by host, operating system, application, data, network devices, and links. This assessment provides vital information for determining appropriate risk levels for each asset and the maintenance requirements for maintaining each one to the desired security level and should be incorporated into the security policy.

- State would mandate to define security zones at the SDC and set security levels for each zone: These separate the data center into areas that are logically separated from one another to contain an attack at minimal impact. Zones can support individual applications or application tiers, groups of servers, database servers, Web servers, e-commerce zones, and storage resources. User access can be limited to Web servers, protecting the

application and database tiers from accidental or malicious damage. Communication between applications can be limited to specific traffic required for application integration, data warehousing, and Web services. Zones created at the Storage Area Network can provide logical separation of each application's storage environment across a scalable, consolidated storage network. To achieve this efficiently, firewalls can be integrated and virtualized to provide secure connectivity between application and server environments.

- State would also deploy control access between zones with firewalls and routers. Firewalls provide perimeter control for state-full inspection of connections to and from the data center while blocking access to nonpublic services and hosts through ingress and egress filtering. Routers provide Layer 3 segmentation between zones, inter-VLAN routing, bandwidth rate limiting, and traffic analysis.

- State would need to implement Perimeter Firewall (Separating Internet from DMZ) and Internal Firewall (Separating DMZ from internal network) to increase the defense against vulnerabilities.

- State would need to uses advanced stateful packet and application-layer inspection firewall, virtual private network (VPN), and Web cache solution that enables internet clients to retrieve the static content from the cache by improving network security and performance for both the Perimeter Firewall and Internal Firewall.

- State would implement network IPS for critical network segments. Network IPS is used for analyzing traffic streams to identify and thwart attacks such as DoS and hacker activity. The system alerts the management console and/or invokes an automated response within the network infrastructure to "shun" or block attacks as they are identified. IDS can also dynamically command

firewalls or routers to block packets from identified malicious sources, reducing the effort needed to mitigate the attack.

- State would deploy endpoint protection for critical servers and hosts by deploying Host based IPS. This functionality discovers attacks in progress, protects operating systems and applications, and sends alarms to the management console when an exploit is detected.

3. State would secure the storage network at the SDC. State must consider SAN security as follows :

–Secure the SAN from external threats, such as hackers and people with malicious intent.
–Secure the SAN from internal threats, such as unauthorized staff and compromised devices.
–Secure the SAN from unintentional threats by authorized users, such as misconfigurations and human error.
–Secure and isolate each storage environment from other storage environments even if they share the same physical network.
- SAN should support cloning (creating copy of production disks) onto less expensive disks from which the backup would be performed without affecting the performance of the production disks/LUNs.

II) Data Privacy policy for accessing data

State would formulate a privacy policy statement and place on all relevant Intranets, Internet and Extranet sites. On-line privacy policy statement would reflect approach to data/information privacy that addresses internal and external aspects of best privacy practices. It would need to use separate security policies for each of the shared database from different applications / departments

- State would mandate privacy policy statement in all relevant internal and external documents and press/media. For higher security of the documents they have to be stored a database. The solution should support versioning capabilities to ensure effective and responsible management of the documents.

- Obtaining consent, when appropriate, from individuals for any personal data collection activities that the State declares in its privacy policy. Consent can be obtained by using online forms containing checkboxes or by asking individuals to sign and return a written consent form.

- State would mandate access to the database/production servers and thus access to the data must be in control of system administrator. The root or administrator password must be known to both the nominated representative of user group and system group so that both should agree before making any major changes in the database.

- Other users accessing the server would be provided with captive account so as to confine and control their action.

- Each activity related to delete or update operation on the database even if the nominated authorized person does it must be logged for the purpose of audit trial and the logs must be protected via proper security mechanism.

- Console operator would also be given captive accounts for performing routine and repetitive jobs such as taking backup, doing recovery and generating the accounting reports. They must not be allowed to come on the OS prompt.

- State would need to use enterprise backup software to perform backups onto Automated Tape Library and these tapes should be transferred to a safe place away form the Datacenter to avoid loss of data in an event of disaster.

- State would mandate to have hierarchical layered structure defined for different types of users falling between super users (root user, account holder) and console operator with different access rights for the proper safety of the data.

III) Data Confidentiality

State may allow the Operator to come into possession of highly confidential public records whereupon the Operator shall maintain the highest level of secrecy, confidentiality and privacy with regard thereto.

- Additionally, the Operator shall keep confidential without any disclosure of all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities.

- State shall retain all rights to prevent, stop and, if required, take the necessary action punitive or otherwise against the Operator regarding any forbidden disclosure.

- The Operator shall ensure that all its employees, agents and sub-contractors execute individual non-disclosure agreements, which have been duly approved by the State, with respect to services provided from the SDC.

- The aforesaid provisions shall not apply to the following information:
  (i) already in the public domain; and
  (ii) which has been received from a third party who had the right to disclose the aforesaid information; and
  (iii) disclosed due to a court order.

- The stakeholder of the data/applications and the party using the same should sign a Non-Disclosure-Agreement (NDA) with the State.

- State would formulate the policy of Intellectual Property rights with the concerned line departments while hosting/keeping their data into the SDC with overall control being with the State Government.

IV) Data Protection mechanism from loss

State would implement proper RAID mechanism to avoid loss of critical and comparatively less sensitive data.

- State would use Enterprise Storage Area Network based storage system for critical applications running on different hardware server machines. The SAN Storage system should be capable of Selective Storage Presentation (A feature by which storage volumes designated for access by a specific server would be fire-walled from all other devices on the SAN) and should support heterogeneous environments. The Storage system should also support hot add, hot removal and disk layout reconfiguration without the need to restart the system.

- State would not use common storage system for non-mission critical applications and also for test and development environments.

V) Disaster recovery and business continuity plan

State would establish a Disaster recovery and Business Continuity Plan for State Data Centre considering various approaches/strategies and selecting the best, suiting the State's DR & BCP requirements provided the

recovery location is in different seismic zone. Various Disaster recovery and Business Continuity strategies are elaborated in annexure – 4.

- State would follow best practices for Application, IT infrastructure, Network and Data at the SDC as per the IDC standards.

- State would formulate a backup policy to periodically backup the data from online machine (hard disk) to offline. Database consistency check utilities must be run to verify that the data back up is consistent and can be used confidentially to recover data at the time of crisis. Periodic checks should be conducted on the backup tapes by way of restoration.

- State would advise the SDC operators to apply patches/upgrades regularly on the IT infrastructure including Servers, Operating systems, databases, application related, network equipment and on the storage system protecting the resources from known issues.

- State would mandate to check the health of storage box including functioning of controllers of hard disk and be monitored regularly.

- State would form proper database recovery policy for different kind of failures to avoid even the slightest piece of data being getting lost. To reduce the recovery time of database, the database size should be kept under control by regularly purging the data and archiving it on the offline media, which is not required for online operation.

- State would organize and manage a dedicated contingency planning team. They will develop the detailed work plan and schedule for development of BC & DRP. They will determine which aspects of the services and operation of the SDC are most critical and creates the justification for the overall plan. The preliminary analysis assesses the potential risk and impact on the State's service delivery and operations, identifies recovery requirements and lists

alternative strategies. In case of contingency, the BCP technical support team determines the feasibility of the plan from a technical standpoint and ensures that all critical alternate locations have the equipment and technical support to continue the services and operations.

- State would come out with a clear definition of individual responsibilities, including who has the authority to declare a disaster and initiate BCP procedures.

- State would be ready with a list of contacts of key personal as and when required in case of emergency.

- State would encourage keeping a vital system/software documentation at the backup site.

- State would ask the partners to lay down the procedures for retrieving and restoring information and data from off-site storage facility and be clearly documented.

- State would keep a copy of complete Recovery Plan and steps involved at the off-site (backup site) with authority defined to use this documentation.

- The data replication between SDC and DR site should be done by replicating the transaction logs that would be restored automatically at the DR Site supporting near-realtime data availability at the DR Site

VI) Monitoring and Management of SDC

State would implement state-of-the art monitoring tools. These tools are deployed for centralized policy provisioning, monitoring, and troubleshooting of security components and IOS Software features. This

solution should include event monitoring and correlation to filter alerts sent to the management console. Communication with data center network devices is most secure using an out-of-band network or through a dedicated administration VLAN. It is recommended to encrypt management traffic with SSL, Simple Network Management Protocol (SNMP) version 3, or Secure Shell (SSH) technology.

- State would need to implement management solutions to proactively manage the servers, which would alert the administrator as, and when each service of the data center reaches the defined threshold before the failure occurs on the servers or devices to ensure increased uptime of the Data Center.
- State to deploy solutions to perform automatic patch management to reduce the manual intervention for ensuring that the operating systems and other system software are current, which reduces the impact of vulnerabilities.
- Define polices for periodic monitoring of activity on the firewall server to check for malicious activity
- Define polices for performing periodic health check on the all servers with the Data Center
- State to define Backup and restore policy
- State to deploy Help Desk solution to track and manage the calls logged and resolved
- State to implement antivirus solutions to automatically update to latest anti-virus signature files
- State to perform periodic audits on the State Data Center using a Third party consultant on the following :
    - Security polices define and its implementation
    - Reviewing of the activities performed for management team
    - Reviewing the Access control to the data center
    - Reviewing the Health Check results and the actions taken
    - Reviewing on the uptime of the service to determine the conformance to the SLAs of the State Data Center

- Other important activities that should be managed at the Data Center:
    - Daily maintenance of system configuration
    - Overall security of the network
    - Day to day disk space management
    - Tracking the servers performance and take the remedial and preventive actions in case of problems
    - Proper upkeep of storage media and perform daily backups based on the backup policy
    - Monitor Physical access to the Data Center

VII) Monitoring Access to Data

State would ensure that all IT related infrastructure used would generate granular logs from which information could be derived.

- State would use technologies to harvest such logs and to consolidate & analyze logs generated by such infrastructure.

- State would do periodic analysis of such logs to bring in changes to the security posture to mitigate risks from newly identified threats.

VIII) Data Security while Retiring Data/Infrastructure

State would prepare guidelines to retire any infrastructure. It is to be ensured that the data on such an asset is backed up and is removed from the asset before it is retired. Data that becomes inconsequential or irrelevant due to various factors must be archived using a proper archival mechanism. Data which needs to be destroyed must be destroyed immediately and proper guidelines need to be defined as a process for the same.

IX) Security Audit

The State shall get the security audited by third party expert periodically (once in six months) to ensure and guarantee security of the Data Centre. The audit shall bring out any security lapses in the system and establish that the system is working as desired by the State.

Annexure - 3

Computing Environment Requirements

Computing Environment Consideration	Requirements	Standard Parameters
Server Management	*Monitor critical resources of operating system*	Monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored. Configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/ critical states and escalate events to event console of enterprise management system. Integrate with enterprise management system and support operating system monitoring for various platforms including Windows 2000/2003 and various flavours of UNIX and Linux. Provision exists for performance scoping and trending to provide real time as well as historical reporting, where specified. Provide performance configuration to enable agent configuration to be done from a central point of control, using intuitive GUIs that provide a common look and feel across various platforms in the enterprise. Performance profiles could be defined in this GUI, and, using drag-and-drop techniques, delivered to the various specified machines in the enterprise running performance agents. These agents could then dynamically reconfigure them to use the profiles they receive. The event generated as a part of Server management should go to a common enterprise event console where a set of automated tasks can be defined based on the policy. Events from Network Management monitoring SWAN will integrate together.
Database Management	*Monitor critical resources and parameters of databases*	Proactively monitor various critical relational database management system (RDBMS) parameters such as database tables / table spaces, logs etc. where applicable, using agents on the servers to be monitored. Integrate with enterprise management system and support monitoring of various RDBMS including MS SQL Server and Oracle. Configure the database monitoring agents to monitor based on thresholds. When thresholds are exceeded, the agents would be able to send alerts to event console of enterprise management system. Monitor various database parameters depending on the database being monitored yet offer a similar interface for viewing the agents and setting thresholds. The Database Management function would automatically discover all Sever databases as well as configuration information and store it in the object repository. The Database Management function would be able to enforce sophisticated policies that monitor and correlate multiple events.
Help Desk	*Provide centralized help desk system*	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 web interface console would also offer power-users tips. Provide seamless integration to log incident automatically via system and network management. Allow detailed multiple levels/tiers of categorization on the type of incident being logged. Provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels.

Computing Environment Consideration	Requirements	Standard Parameters
		Each incident could be able to associate multiple activity logs entries via manual update or automatically update from other security tools or system management tools. Provide audit logs and reports to track the updating of each incident ticket. Proposed incident tracking system would be ITIL compliant. It should integrate with Enterprise Management System event management and support automatic problem registration, based on predefined policies. It should be able to log and escalate user interactions and requests. It should provide status of registered calls to end-users over email and through web.
Web Management	*Montor critical web servers*	Web Server Management. The Web Servers would be proactively monitored for the availability, health and performance of Web servers. The Web Management would automatically correlate the status of Server, Services, Disks, Invalid URLs, Polled URL Counters, Server Health, Polled Counters, Polled Events, and would provide alerts to the Web administrators. The alerts could also be integrated with Help Desk Management for efficient call tracking and problem resolutions. Web Response Monitor. The Web Management would also provide capabilities to monitor and proactively alert Web Responses on availability, health, and performance of one or more Web sites and services from the perspective of a user attempting to access the site. The Web Management would use combination of HTTP and FTP to determine the availability, round-trip response, and content for select web sites. Web Traffic Analyser. The Web Management would analyse the traffic and provide simple and easy to understand reports in tabular or graph formats that show statistical, demographic and trends in the performance and use of internal web sites. The Web Management would provide reports on the central. Provides integrated management of Web server and components.

Security Requirements

Security Consideration	Requirements	Standard Parameters
Network Security	*Minimal deployment of the following baseline controls on all network devices*	Use of login Banners at login time Network traffic filters and Access Control Lists to restrict unauthorized traffic Strong authentication mechanisms for all console or remote administrative access Firewalls to permit only authorized traffic Controls to ensure the integrity and confidentiality of the appropriate Domain Name Server data Use of network based intrusion detection tools Use of digital certificate verification between server/sever and server/client • Use of Virtual Private Networks or equivalent
Anti-Virus	*Maintain anti-virus measures*	Host and Web based Inbound and outbound monitoring on all data transfer mechanisms and all e-mail systems Early virus alert service from vendors Real-time on-line access scanning Timely updates to signature files and search engines Common solution for antispyware and virus infections. Integration capabilities with security management solution for management and monitoring. Heuristic scanning to allow rule-based detection of unknown viruses 100% certified to protect against “in the wild viruses” by the ICSA
Host Server Security	*Deployment of baseline controls on all host servers including detail description of operating/file system controls used to secure servers and access controls (authentication & authorization) on servers, platforms and databases*	Review all default settings Strong access control lists to restrict unauthorized access Remove unneeded network protocols,services, default or system user accounts, and any sample application code Resetting of default passwords (includes periodic password resets) Use of dedicated servers as required Super user rights i.e. Administrator for windows and root for Unix should also be contained to them limit of those IDs not able to logs residing on the Operating System

Security Consideration	Requirements	Standard Parameters
		Use of partitioned servers as needed Provision for an Identity to be auditor with access to only logs and read only rights to configuration. This is to ensure that super users of Operating systems doesn't have access to logs. Delegation of rights like maker, checker and auditor with one Identity having access to formulation of policy but not implement it , second identity having access to delpoyign policy but no access to define policy and auditor with access to logs. Program pathing to enable access to data on server thorugh a allowed application only with ability to define access based on time and day of week. Provision for a warning mode that can be used during implementation to verify policies and their impact before deployment. 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. Must be able to prevent hackers with root access from circumventing or shutting down the security mechanism. Must use a self-protected database for storing all security information. STOP (Stack Overflow Protection) to prevent stack overflow exploits on systems, to ensure that arbitrary commands cannot be executed in order to break into systems Other measures as recommended by the OS vendor
Identification, Authentication and Authorization	*Restrict electronic access to the Web site or application beyond user level access to only authorized persons.*	**Security Controls** The users are uniquely identified and authenticated by the systems. The use of any form of generic or shared user identifier is expressly prohibited. User-level access enforce by the "least privilege" principle (i.e. Users/Application Administrators *only* have the level of access to the system required to perform their job functions.). Use of strong industry standard encryption technology (e.g. 3DES or Blowfish) to encrypt l data identified by the States as per data classification (e.g. "sensitive" or "confidential". A common security layer for all application reducing the time to launch new application and mantaining secuirty. The security layer should be abel to integrate with all industry leading authentication mechnaisms.

Security Consideration	Requirements	Standard Parameters
		The security mechanism should not run as a process or service which can be killed or stopped to allow access to entire infrastrucutre. Policy information should be stored directly in LDAP, so that a single directory can be used to store both user and policy information. Aplications should use a central LDAP, NT, ADS , SQL DB as authentication directory For web based application the cookies should be 128 bit encrypted and session management capabilities should also be built in common security layer. Administrator should be able to specify that a certain directory be used for user authentication, but a different directory be used for user authorization.Option should allow multiple directories to be configured. Following password management features should be part of common security layer **Management of Passwords:** Passwords changed at least every 45 days Default passwords changed immediately upon account creation Password file must be encrypted and secured Ten (10) unique passwords within a password history cycle Password length at least 6 characters Use of strong password structure (Ex: “Pa33WorDS”) Password measures enforced automatically Management of User Accounts: User accounts and passwords audited every 90 days for compliance Accounts disabled or locked after 3 failed login attempts within a 30-minute period. Locked accounts re-enabled by authorized system or security administrator Verification information for resetting passwords selected by Client Time-out feature for inactivity Inactive user accounts purged after 90 days
Data Transmission Security	*Safeguard the confidentiality and integrity of all data being transmitted over any form of data network.*	Strong, industry standard encryption for the data identified as 'sensitive' or 'confidential' as per data classification.(Examples include SSL for Web browser sessions, or PGP file encryption for bulk data transfers.). Secure Socket Layer (“SSL”) or stronger encryption techniques for network access via the public Internet. Strong industry standard tools for monitoring, controlling, and administering electronic transmissions.

Security Consideration	Requirements	Standard Parameters
Firewall Services	*Use of firewall tools and services in accordance with the Data Centre requirements, policies and procedures, including general maintenance and monitoring of firewalls and implementation of firewall rule set changes.*	Controlled implementation and scheduled maintenance of firewall rule set changes Active monitoring to identify attempted or actual security violations Controlled emergency maintenance of firewall rule set changes Two (2) business day turnaround time for firewall rule set changes
Intrusion Detection and prevention Services	*Use of intrusion detection/prevention tools to detect unauthorized access to or unauthorized activity on the networks, computer systems and network devices associated with the State Data Centre.*	Network and/ or Host based Active monitoring to identify attempted or actual intrusions Timely updates to signature files
Security Monitoring	*Provide monitoring services*	Real time monitoring of all systems and network devices/systems to detect potential security violations. Such monitoring will include but is not limited to operating system access, detection of unauthorized processes or software, unauthorized modification of existing software or data, or unauthorized configuration changes to computer systems and network devices. It will also include the logs of all firewalls, intrusion detection/prevention systems, physical access controls or other security-related systems. Retain the logs of all security-related systems, to include but not limited to firewalls, intrusion detection systems, access control measures (both electronic and physical) and file integrity checker logs for forensic or evidentiary purposes.
Incident Response	*Reporting of any and all security incidents*	Security Incident Response Plan acceptable to the State Government Log of security incidents must be maintained and classified as confidential and proprietary property of the State Government Incident Report and Action Plan per incident

STORAGE REQUIREMENTS

Computing Environment Consideration	Requirements	Standard Parameters
Backup	*Provide centralized online backup for mission critical applications*	Proposed Backup Solution should be available on various OS platforms such as Windows and UNIX platforms and be capable of supporting SAN based backup / restore from various platforms. Proposed backup solution shall take backup of databases. Proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration. Backup software should support backup to disk that allows users to use disk technology as an intermediate step in the backup process. This allows faster access speed and higher reliability of disk technologies ensures reduced backup and restore time as well as higher success rate for backups. The proposed Backup Solution should support the capability to write up to multiple data streams to a single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the Drives using Multiplexing technology. The proposed Backup Software shall offer OPEN File Support for windows and Novell Netware. The proposed Backup Solution should have 'Hot-Online' backup solution support for different type of Databases such as Oracle, MS SQL, etc. Backup software should create a media index (catalog) file on your media to improve performance for merge jobs and database backup jobs. Backup software should provide command line utilities an alternative method of accessing the operations available from the GUI Manager. Backup software should also provide report writer that allows designing of report templates which can be used to generate meaningful reports in Comma Separated Value (CSV) or extensible Markup Language (XML) format.
Storage Resource Management	*To manage and monitor storage resources effectives distributed on SAN/ NAS*	Discover the infrastructure and monitor file system devices Understands application, server, and subsystem performance and availability Capacity management: Collects physical (configuration and information) and logical (volume space) information of SAN components, which shall be used to generate reports.

Computing Environment Consideration	Requirements	Standard Parameters
		Configuration Management: The ability to monitor the storage for applications based on capacity and performance. Event Management & Reporting: Problem notification for storage administrators, reports generation for daily activities, real time reports for SAN environment Policy management: Dictates storage policy and enacts actions on hardware, files, users, etc Shows the components, affected servers, applications Should provide detailed reports on storage access and usage pattern

Annexure- 4

1. Data Centre Manager (Project Manager) – 1 No. : Responsible for overall management of the Data Centre, user SLA commitments, performance, availability, response time, problem resolution etc. He/She should also be responsible for effective Resource management, System & Resource planning based on business forecast and would be the single point contact for managerial responsibilities and direct interface with State IT head. Data Centre Manager should have capabilities in team management, capacity planning and process documentation.

   The desired profile of the candidate should be minimum B.E. (Computer/E&C/Electrical)/MCA preferably MBA with 6-8 years experience. He/She should have exposure to BS15000 process /ITIL or ITIL certified and have a proven track record of managing operational IT support teams including establishment of RMC /processes, technology & Staffing. PMP Certification is a plus.

2. Database Administrator – 1 No.: Responsible for Data Base Administration, Web Administration, Application Hosting, Web Designing, Staging and other related services. He/She should also be responsible for database and application change management procedure.

   The desired profile of the candidate should be B.E.(Computer/E&C)/MCA with 3-4 years experience in administering production data bases and worked in Oracle 9i, 10g, DB2, MS-SQL etc. Knowledge in PL/SQL Programming with experience in handling standby databases preferred. Must have technical certification in Data Base Administration.

3. System Administrator – 1 No.: Responsible for OS administration / management, database configuration, scalability, performance, load-balancing, troubleshooting & debugging and monitoring of servers. He/She should implement the back-up plan for storing and retrieving of

data, maintain servers, machines, printers and also responsible in resolving the real time (RT) requests raised by users as per SLA.

The desired profile of the candidate should be B.E. (Computer/E&C)/MCA with 3-4 years experience in sys admin of RDMB data (MS-SQL, Oracle etc.), sysadmin windows-2000/UNIX/Solaris etc. server, programmer of Java, C, C++, SQL,PL/SQL, Corba etc. Technical certifications on Oracle/SQL/SUN products etc. is must.

4. Network Support Staff – 2 Nos.: Responsible for network uptime, security, performance, monitoring and other related services. The candidate should be well versed with Routing and Switching devices and technologies like ATM, Frame Relay, MPLS, Wireless, Broadband and Protocol Analysis Tools. Must have beginner to intermediate skills in Information Security technologies like Anti-virus, Firewalls, 2 & 3 factor Authentication, IDS, IPS, Content Filtering, Encryption, VPN, Threat Management and be familiar with Information Security Audit parameters.

   The desired profile of the candidate should be B.E. (Computer/E&C)/MCA with 3-4 years experience as mentioned above. Certification like CCNA/CCNP/PIX/CCSA would be preferred.

5. Technical Support Services – 4 Nos.: Responsible for L2-support, H/W &S/W support and would provide help to the Data Centre Operations & Management Core Team in quick resolution of problems. The technical support team would work on shift basis and ensure uptime of services. He/She should be responsible for escalating the call to the specialized domain and closely work with the domain experts and do the first level of analysis once call is logged by the help desk support team and ensure uptime of services through NMS and generate reports to meet the SLAs signed by the States with different stakeholders.

The desired profile of the candidate should be minimum Diploma/B.E. (Computer/E&C) with 2-3 years experience in technical support services/ operations , IT Infrastructure, managing & updating customer database with pleasing personality and good communication skills. Technical certification like CCNA etc. preferred.

6. Help Desk Services – 2 Nos.: He/She should be capable of complete call management process with standard call logging and escalation tool. The requirement of manpower for Help Desk Services may increase as demand grows and more services are added to the State Data Centre.

The desired profile of the candidate should preferably be Graduates/Diploma holder in Hardware/Networking with good communication skills and proficiency in English and local languages.

7. Administration/HR – 1 No.: The persons recruited should be responsible for entire Data Centre administration, Logistic support, procurement, Stationery, administrative co-ordination etc.

The desired profile of the candidate should be Graduate with Masters/ PGD-HR/PM/IR with 2-3 years working experience in the administration / recruitment / logistic support of manpower and worked either with Data Centre operation or with an IT/ITES industry with good communication & HR management skill.