

State & District Data Centres

1 BACKGROUND AND EXECUTIVE SUMMARY

1.1 Vision and Objective of Punjab Government

Punjab Government is committed to providing a responsive and effective administration for the welfare of the public keeping in view the national objectives. Punjab Government recognizes the need to harness the growing power of IT for the betterment of the life of the residents of Punjab.

The vision of Punjab Government is to create a knowledge-based society through extensive use of Information Technology. Punjab Government envisages a scenario wherein every citizen shall be able to access the benefits of Information technology by the year 2007. The ultimate goal is to use I.T. as a medium for effective interaction between the Government and the public so that exchange of information and access to government departments is speedy and easy, leading to a better quality of life.

Punjab Government is committed to provide for better **public service** to its citizens through e-governance which is efficient, speedy, simple and cost effective. It has been decided to establish one state data centre at Chandigarh and 19 district data centres at district levels.

1.2 The project Sukhmani- Integrated Services

Project aims to bring together all the departments under one single umbrella and give citizens of Punjab a “multi-service” – “single-window” experience.

The key objectives are to

- Provide for hassle free one-stop solution to the citizen
- Minimize multiple interaction points for the citizen and hence reducing the wastage of valuable time
- Provide for better turn around time in receipt, processing and issue of services

This Project is a Department of IT initiative in collaboration with other departments under Punjab Government. The aim is set up an integrated chain of Sukhmani Centres in Punjab and a comprehensive and transaction based Citizen's Portal.

For setting up the Sukhmani Centers, the Government of Punjab has set up a pilot Sukhmani Centre at Ludhiana which has started its services successfully since November 2004.

1.3 Local Area Network, Wide Area Network (PAWAN) and State Data Centre

The Department of Information Technology of the Punjab Government has initiated the process of deployment of IT in many elected departments and creating Local Area Networks within the departmental offices and setting up a Wide Area Network (PAWAN) across the state for inter departmental connectivity. In a time bound program personal computers/ laptop machines are being provided to senior government officers. Punjab Civil Secretariat would also be linked with all departments at other locations in Punjab using PAWAN. The area where large deployment of IT has been undertaken includes the following:

- Excise & Taxation
- Transport
- Treasuries & Accounts
- Local Governments
- All DC offices
- Labour & Employments
- Advocate General
- Agriculture
- Social Security
- Printing & Stationary
- Animal Husbandry
- Food & Supplies
- Public Health
- Languages
- CM Office
- Rural Development
- Vigilance Department
- Civil Defence and Home Guards
- Punjab Civil Secretariat
- Chief Architect
- Forests & Wild Life
- Punjab State Electricity Board
- Digitization of Land Records
- Multi Service Smart Cards for Citizens
- Punjab Property Registration
- Digitization and Storage of Records

In addition to it, the Punjab Government is proposing to set-up a data center for the Government and inter-connects with the proposed Sukhmani centers/ CSC centres to be set up under the scheme of Government of

India by 2007. The following shows some of the important applications already been deployed by the Government:

- Suwidha- DC office Services already implemented at 17 districts and 72 SDM offices
- Sukhmani- Provision of integrated Citizen Services
- Transport Services – Vehicle Registration and driving licenses being rolled out in Punjab
- Social Security- old age pension completed in entire state
- COSTISP- Computerization of Sales Tax Barrier based on VAT completed
- PGPMS- Database of 3.5 lac government employees being created
- Computerization of Land Records being rolled out in the state
- PRISM- Property Registration completed in Sangrur district
- MSC- Multi Service Cards- District Fatehgarh Sahib being completed
- Treasury Information System- Completed in state at District and subdivision level
- School Education- under ICT grant from GOI
- Labour & Employment-under implementation
- Process Re-engineering of District HQ- study complete, recommendations being implemented at Jalandhar and Patiala districts

2 District Data Centre Objectives

As an imperative of the e-government roadmap, Punjab Government intends to provide services on the Internet to the citizens in a secure and controlled manner in addition to the Sukhmani centres/ CSC Centres. These services must be consistently available and have the capacity to grow, as business requirements increase. With the falling costs of communication, centralized architecture has become a reality. This has resulted in need for a facility that provides a platform for effective management of information assets being created by government, as a part of its e-governance initiatives.

To meet these objectives, Punjab Government requires a Data Center in each of its 19 districts as an intermediate network between the open Internet and the private government environment. This would enable the government departments to locate their IT Infrastructure at the same location leading to ease of integration and efficient management, ensuring sharing of bandwidth and computing resources to meet the peak load requirements of individual departments.

At the outset, the District Data Centers would be able to provide the following:

- Various hosting options
- Standard technologies
- Guaranteed service levels
- High quality support, operation and monitoring of departments' applications
- Data and Application availability seven days a week twenty-four hours per day
- Centralized network management and operations capability
- Facility for centralized management of enterprise client/server systems
- Custom Security options, Multiple security levels
- Backup and Archival Services
- Comprehensive Disaster Recovery

3 District Data Center Plan & Methodology

The Punjab Government plans to host its district data centers in its own premises in the District Administrative Complex, wherein the servers would be procured by the individual departments and the Department of Information Technology will invest on the data center hardware required for operation of the Sukhmani Centres/ CSC Centres. The Government also plans to provide common IT infrastructure services to the departments in this central facility. These include

- Managed Services
- Value Added Services
- Security Services
- Physical
 - Logical – Network and Host
 - Storage Services
 - Primary Data Storage
 - Tape and Disk Backup
 - Disaster Recovery/Business Continuance
 - Mail Services
 - Centralized Mail Server envisaged for all departments

3.1 The Data Center Requirements

The broad requirements of proposed data center are as follows:

- Establishment of Data Center **Facilities Infrastructure**, including:
 - Raised Floor
 - Electrical – Power, UPS and Diesel Generators for backup
 - Fire Detection and Suppression
 - Humidity, Ventilation and Air Conditioning(HVAC)
 - Natural Environment Handling
 - Physical Security
 - Access Control Mechanisms
 - Data/Telecom Cabling

- Alternate Data Storage establishment
- Installation and Integration of the **IT Infrastructure**, including:
 - Servers
 - Network – active components - switches, routers; passive components - backbone
 - Racks
 - Telecom equipment and Connectivity including bandwidth, etc.
 - Integrated Portal and Integration with the departmental information systems
 - VSAT connectivity for redundancy/ Disaster Recovery
 - Enterprise management systems
 - Network Management Systems
 - Storage – primary and secondary (implementation of DAS/NAS or SAN)
 - Security – Firewalls, IDS, VPNs etc.

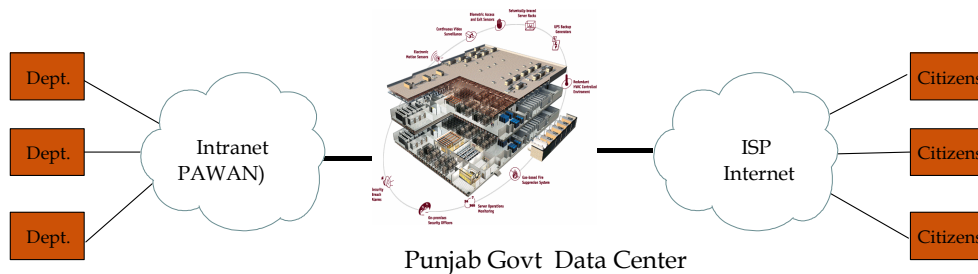
4 District Data Center Design

The requirements as envisaged by the Punjab Government are as per Annexure A.

5 The Data Center Logical Design and Requirements

5.1 Logical Design of the District Data Centers

As part of the Sukhmani/ CSC project Punjab Government portal will act as a Citizen interface through web with the Government. The Sukhmani Centers will also use the same portal for its integration with the



departmental information systems.

Then as a next step, the Department of IT proposes to create an integrated center at District level to host all information system assets of the government and this proposal addresses the requirements of both the Portal and the next phase activity of consolidating the information assets at the data center.

5.2 Data Center Investment Requirements:

The Punjab Government has identified the following as requirements for the proposed data center for the purpose of the budget proposal. The rest of the requirements will be met through internal budgets of the departments over a period of time.

Civil & Electrical Requirements:

- Raising Floors
- Alternate Power Supply mechanisms like DG Sets, etc.
- The fire Suppression Measures
- The furnishings
- Air Conditioners
- Physical Access Devices
- UPS
- Electric Wiring and LAN Cabling
- Civil Work to reconstruct the allocated space
- Storage Cabinets and Fire proof cabinets

Information Technology Hardware:

- Web Servers
- Application Servers
- Storage Servers
- Monitoring Devices such as Key boards Monitors, etc.
- Printers
- Desktops
- Backup Devices
- Redundant Servers for DR
- Servers for Firewall, IDS, access control systems, etc.

Networking Equipments

- Routers at all Departments
- Central Router
- Redundant routers
- Hubs and Switches
- Networking Monitoring Devices
- WAN Switch
- Internet Router
- Server Racks

Software:

- Windows Servers
- Linux servers
- SQL Database licenses
- Oracle Database licenses
- Firewall

- IDS
- Network Monitoring Systems
- Unix Servers
- Redundant Firewalls
- Web Server Licenses
- System Software
- Office Automation tools

1 The Data Center Design

The design of modern data centers (DC) represents many challenges. Each step in the evolution from mainframes to mini-computers to servers has brought with it specialized building design criteria and equipment requirements.

The extent to which a data center must remain operational even when some of its resources are impaired or unavailable will greatly influence how the following design objectives are implemented:

- **Availability:** The probability that a service will be ready to perform its primary function when needed
- **Backup:** The degree to which a function may be duplicated by an alternative system or process
- **Redundancy:** The degree to which the functional aspects of a system or process are duplicated
- **Survivability:** The degree to which a system or process can fail and still perform its intended function, albeit at reduced capacity

Punjab Government plan to have a flexible physical infrastructure to support its future needs and the expected changes.

The detailed requirements as envisaged by the Punjab Government are given in the following sections:

1.1 Data Center Infrastructure Specifications Requirements

1.1.1 Facility Infrastructure

1.1.1.1 Locational Aspects

Site Safety: Site should be free from Natural Disasters like flood plains, tornado or hurricane hot spots or seismically active areas. It should not be near source of Electromagnetic Interference or Radio Frequency Interference like telecommunication signal facilities, airports, electrical railways etc. It should not be near sources of Industrial Pollution. Site should be free from Vibration sources like airports, rail lines, busy highways, traffic tunnels, mines etc. Preferably facility building should be within an existing complex to take advantage of established security measures and to protect data center from vandalism, industrial espionage, or terrorism. There should not be exterior windows in the data center to avoid crime targets like vandalism shooting and no proximity to neighboring structures which are industrial in nature to avoid fire hazards.

Emergency Services: Adequate access should be there for support and emergency services. Redundant utilities feed and good infrastructure support is required.

1.1.1.2 Floor Layout

Floor layout is almost always a trade-off between security, rack density, the future growth expectations, and manageability. An illustrated lay out is given below

The Punjab Government proposes to establish a four level of floor layout in order to provide adequate security as well as managing the infrastructure.

1.1.1.3 Electrical

Power Supply: Power supplied to each area will be terminated in a main distribution panel. Ideally, each area will have power distribution units (PDUs) within each technical suite. Special consideration will be provided if special power requirements such as additional sockets or DC (direct current) supplies are required.

Main power to the data center will be supplied by the regional electric power utility. To reduce reliance on one feed, separate feeds into the building will be made. Once inside the building, the power will be distributed via at least two means to the individual technical suites and other protected areas.

At a minimum, two-fold resilience will be provided in the form of uninterruptible power supplies (UPS) to each area or neighborhood. Additionally, diesel generator backup will start automatically within seconds after a main power source failure.

UPS and DG backup: A DC will incorporate two levels of redundancy in its power systems. In addition, it also requires deployment of UPS systems with hot standby redundancy, through which the raw power (from the primary/alternate electricity provider) is channeled to ensure a longer installed life of equipment. The UPS system will be backed up by batteries to provide at least 30 minutes of continued power supply. The UPS and battery system will be backed up by high powered Diesel Generators ('DG sets'). The DG sets will be equipped with an Auto Mains Failure (AMF) system to ensure instant startup in case of a power failure. The DG sets, capable of taking the entire load of the DC (servers, air conditioning etc), provide uninterrupted electricity.

1.1.1.4 Fire Detection and suppression

The building will be protected by a fully automated fire detection and suppression system before damage occurs. All technical suites will be equipped with FM200 (or equivalent) gaseous extinguishing systems, to provide rapid discharge and flame suppression in the event of a fire, while minimizing damage to equipment and reducing danger to personnel. State-of-the-art smoke detectors, heat detectors and a fire management panel will be used as part of the fire detection and extinguishing system.

An automatic detection and extinguishing system shall be installed in space below the raised floor. The server Hall shall be separated from other occupancies within the building by fire-resistant rated walls, floor, and ceiling constructed of noncombustible materials.

The data center will comply with the National Fire Protection Association (NFPA) 75 standard for the protection of electronic computer/data processing equipment.

1.1.1.5 Humidity, Ventilation, Air Conditioning (HVAC)

Equipment performance and life span can be significantly improved by housing the system under optimum environmental conditions.

The air should be controlled and monitored with an Environmental Monitoring / Alarm and Paging System. Criteria in determination of the air conditioner placement should be its effectiveness in addressing the current planned load, and their adaptability to change in configuration. There should be no air-conditioning ducts under raised floor or inside the false ceiling.

1.1.1.6 Natural Environment Handling

The exterior of the building will be protected against lightning to avoid transient high voltage and EMI. Server Hall will be isolated from contaminants. Inside server Hall airborne dusts, gases and vapors should be maintained in the defined limits to minimize their potential impact on the hardware. Server Hall will be free from water ingress.

1.1.1.7 Physical Security

Physical access to technical suites and other areas of the building will be controlled and monitored on an ongoing basis to maintain and control access to restricted areas. Access to the server hall will be strictly regulated, and limited to only those personnel who are necessary for its operation.

1.1.2 IT Infrastructure

IT Infrastructure will be installed keeping the following features in mind:

Redundancy: To achieve maximum availability and uptime, mission-critical web sites and data storage requires high redundancy. A backup should be ready for immediate implementation for any failure in any connection related to network functionality. Without redundancy in design, network is vulnerable to a wide range of problems that could have grave ramifications both for Punjab Government and the data centre.

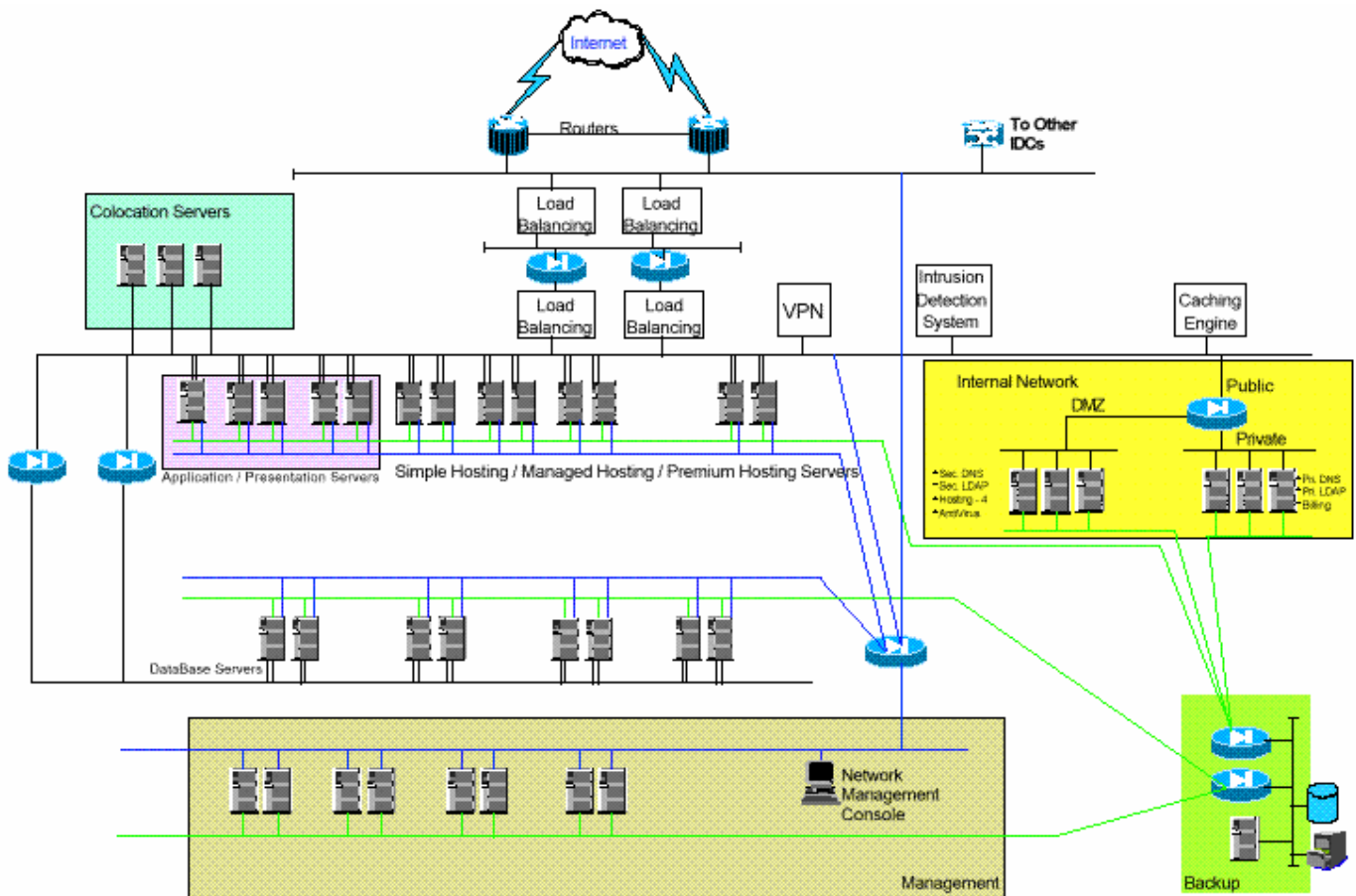
Availability: High availability should be present in many layers of the hosting services with the intent of ensuring maximum accessibility to content and stored data.

Scalability: Data Center should ensure that increased traffic flow and demand for services does not affect applications. Network should therefore be scalable to meet the sudden surges in traffic.

Security: Security is a major consideration for the Data Center network infrastructure. Businesses must be assured of not having to worry about security breaches, both physical and virtual, thereby safeguarding the applications and preventing loss of business.

1.1.2.1 Networking Architecture:

The data center network is divided into 4 layers of functionality depending on the service provided at each layer. The layers in a broad sense are described as follows:



The **Border Layer** is the boundary of the data center to the external world. It is the layer from which traffic from the external world flows into and out from the data center using BGP and protects the IDC from denial of service attacks.

- The **Core Layer** does fast packet forwarding.
- The **Distribution Layer** aggregates traffic from various customer access switches and applies policy for individual IDC customers.
- The **Access Layer** with access L2/L3 content switches that provide connectivity to the data center servers.

Network architecture will focus on the following requirements:

- All firewall systems will be redundant and have real-time fail-over capabilities.
- All LAN routers and switches would provide redundancy capabilities.
- All WAN connections to provide alternate routing paths.
- All network components will be monitored using monitoring software and protocols. Critical network events will be defined and configured on the devices. Critical system messages will be reported to the NOC in real-time.
- Cold standby network hardware (routers, switches) will be available to replace existing components in the event of a hardware failure.
- Systems running critical services will at least have one duplicate per physical location.
- Load balancing hardware will be implemented to distribute network traffic efficiently and effectively to critical production servers.

1.1.2.2 Security Architecture

All connections from public and external partner networks to the Data Centre network will be limited to authorized connections only. The network architecture will provide mechanisms to ensure confidentiality and integrity of systems and data, with control measures in place, to detect suspicious activity in a timely manner.

The network security policies and standards apply to the following network resources:

- Routers
- Switches
- Firewalls
- Network management stations
- Network services (DHCP, DNS, other services enabled by Network Management Software)

Some of the important requirements w.r.t. network security that will be addressed as part of implementation are:

- All hosts and networks will be protected with firewall mechanisms to prevent unauthorised connections to IDC network and systems.
- Hosts that require access from untrusted networks, e.g., WWW servers, will require firewall mechanisms using DMZ architectures.

- Only hosts on a DMZ network may, if required, connect to internal systems. The DMZ network and internal network will be separated using firewall mechanisms. Hosts from untrusted networks may never connect directly into the internal network.
- All hosts and network systems will be configured with adequate access controls to limit access from untrusted networks (Internet and DMZ).
- Hosts on the DMZ will only make connections to the internal network after design review and formal approval.
- The amount of information available via networks or hosts will be limited to the extent possible.
- User access from public networks into the IDC network will require strong authentication (something more than just a <username:password> like e.g., secure IDs) and their sessions will use VPN technology to ensure the identity, authenticity and confidentiality of the data transmitted.
- Extranet networks will connect through a dedicated firewall infrastructure. They will not be allowed to connect directly into any production infrastructure. Access to IDC internal resources should be limited to the extent possible.
- Access to systems containing highly sensitive data (e.g., application data, user details etc.) will be protected with firewall mechanisms.
- All firewall systems will at a minimum report critical system events to a log server. The log server should have adequate access controls to prevent unauthorized access to log files.
- Network segments providing access to IDC web resources (e.g., external and DMZ segments) will be provided with Network Intrusion Detection Systems to detect suspicious network activity and alarm IDC system owners in real-time

Besides the above, all network architecture components should provide sufficient redundancy to ensure continuity in the event of a network (component) outage. Additionally, network mechanisms should provide load-distributing capabilities to ensure efficient and effective network traffic management.

1.1.2.3 Storage Architecture

The goal is to reduce data redundancy, increase data availability, ease and enhance the scalability of data storage, while improving serviceability and reducing overall costs by simplifying data management.

General requirements:

- Primary Storage: RAID protected storage outside the cage. Storage equipment should be linked from the Punjab Government's systems to an external SAN in the Data center. However, Punjab Government will evaluate the need for Storage Area Network at the time of project implementation, through its being envisaged as part of the project proposal.
- Tape and Disk Backup: One full backup, plus six incremental backups of the data per week will be performed or else the backup regime will

- be in accordance with the individual department's needs. Restoration and off-site tape storage should be available on demand
- Backup solution will have the following features:
 - Performance, Availability, and Safety
 - Flexible Implementation
 - Heterogeneous Support
 - End-to-End Integration
 - Secondary Storage:
 - Need reliability to provide continuous access to critical data
 - Performance must match throughput of very large servers
 - High capacity for backups and archiving
 - Effective tools for busy system administrator
 - Disaster Recovery/Business Continuance: This service should include remote backup, disaster recovery audits and business continuance planning (also included as a part of performance optimisation services in the next section)

1.2 Data Center Services Requirements

As per the requirements of its individual departments, would be providing the following services from the data center:

1. Hosting
2. Application and Infrastructure Management
3. Performance Optimization

1.2.1.1 Hosting

The data center should be able to provide the following hosting services:

- *Co-located Hosting*
- *Shared Hosting*
- *Dedicated Hosting*
- *Managed Hosting*

As per its requirements, the Punjab Government would choose the appropriate hosting option for its individual departments.

1.2.1.2 Application and Infrastructure Management

The following services are proposed to be provided to the individual departments:

- a. Infrastructure Management** – managing and monitoring the server and the network infrastructure
- b. Application Management** - monitoring and management of 3rd party package and custom applications, ranging from basic call handling and troubleshooting to patch management and full source code control
- c. Managed Security Services** - managed offerings for customer firewall, intrusion protection, and VPN requirements based on a best-of-breed cross-vendor approach
- d. Managed Storage Services** - managed primary disk, remote mirroring and tape back-up with onsite or offsite storage options

a. Infrastructure Management

The infrastructure monitoring will focus on the following:

Server and Network Monitoring

The server and network monitoring services will include real-time metrics available over web. Standard services should include:

- CPU usage monitoring
- Data transfer monitoring
- Memory monitoring
- Disk - Allocation/Management/Maintenance
- NIC Monitoring
- SMPS health Monitoring
- Fan Monitoring
- File-system monitoring
- System Log Analysis
- Web Server log analysis
- Web response monitoring
- Bandwidth: 24x7 monitor that will record DC's Internet traffic utilization

Reports

Performance reporting of business critical machines works in tandem with the system activity reporting utility of the operating system and it collects various performance metrics and presents easily understandable graphs, which can be used by administrators to analyze performance issues/bottlenecks. It also helps in capacity planning by giving prior indications of potential bottlenecks. It includes reports on:

- CPU Performance
- Bandwidth Utilisation
- Browser Behavior Pattern

b. Application Management

Application Management service deals with the total management of the business application, from the network, systems, security, and storage infrastructure to the management of application level components. Application Management includes application monitoring and load / stress-testing to source code management.

c. Managed Security Services

A secure infrastructure is key to a successful business. With the rapidly changing world of network security and the ever-increasing incidents of hackers, worms, viruses, employee sabotage and more, the data center need the best security possible. The data center should provide the following security services:

1. Basic Security Services

- Firewall
- Intrusion Detection
- Antivirus
- Denial of Service

2. Advanced Security Services

- Server/Operating System Hardening
- Incident Handling
- Penetration Testing
- Patch Testing
- Vulnerability Analysis

d. Managed Storage Services

Managed Storage Services should provide high performance primary data storage and cost effective tape backup services both of which are key components within the business continuity arena. Mirroring and Storage on Demand services can also be considered by the Government as per its requirements.

1.2.1.3 Performance Optimization

Performance Optimization services are targeted at providing its departments with decreased end-user response times and enhanced redundancy and failover capabilities for maximized application availability and performance. These include:

- a. Availability Services*
- b. Load Balancing*
- c. Intelligent Caching*
- d. Content Delivery & Streaming*
- e. SSL Acceleration*
- f. Business Continuity/ Disaster Recovery Services*