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