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.