INFORMATION TECHNOLOGY DEPARTMENT
GOVERNMENT OF ASSAM

INFORMATION SECURITY

Controls & SOP

Introduction

Security of systems managed by the Department/Organisation is highly important as the Government has declared some of its asset as critical government infrastructures. Confidentiality, Integrity and Availability of the systems and data shall be maintained at all times through controls that are commensurate with the criticality, so as to protect it from all types of threats - internal or external, deliberate or accidental. The purpose of the Information Security Controls & SOP is to outline a cyber-security framework that the Department/Organisation can apply, to protect their systems and data from cyber threats as per ISO 27001:2013 standard.

Organisation must ensure to follow below guidelines in their Information Security policies for their Organisation/ Department information security Program.

Human Resources (Third party)

- The background verification needs to be made by the Department/Organisation for all personnel employed in the IT projects. This may include all vendors, consultants and s, O&M firms, and service providers appointed by the department/organization.
- The department/organisation shall arrange training for the employees to keep them updated on information security.
- A termination process shall include returns of all issued assets that are the property of the department/organization. User ID, credentials and access rights shall be revoked/ deactivated at the end of the last working day

Access Management

- Only authorized users shall be granted in the network, application, database etc.
- Role based access must be exercised and access must be given only need to know basis and least privilege mechanism.
- User login to the network shall be controlled /monitored
- Organization must maintain accounting and audit trail log monitoring system.
- Strict password management policy should be adhered:-

General Password Construction Guidelines

Strong password has the following characteristics:

- Must contain both upper- and lower-case characters and digits, special characters as well, at least eight alphanumeric characters long,
- Must not a word in any language, slang, dialect, jargon, etc., Not based on personal information, names of family, etc.
- All system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.) shall be changed on at least every 90 days

Assets Management

- The department/organisation shall prepare an IT asset register to documents all the information assets such as all PCs, laptops, Phone, Printer, Network devices, Firewall, Storage, all web portal, application along with the details of Vendor, Model number, Serial Number, against the AMC partner and the exact location of the device. Organization should update it a regular interval for any addition and deletion of assets. s.

Physical and Environmental Security

- Datacenter, Network Operation Center (NOC) room shall be identified as restricted area and applicable security controls should be applied and monitored.
- All equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities by using online UPS and Generator.
- Only persons authorized by department/organisation shall be allowed to enter the facilities by showing valid identification.

Operations Security

- Standard Operating Procedure (SOP) shall be developed every time new information system or services are introduced.
- Any changes in system/application including patch update, modification/enhancement update/release must be tested in Test environment before moving into production.
- Information security aspects may be analyzed for any change.

Patch Management

- Patches to the production systems shall be applied as per OEM's (Original Equipment Manufacturer) instruction to ensure that the systems are protected against the threats from the spread of viruses, worms and malicious activities to an acceptable level
- Proper backup of the system shall be taken before deploying the patch to ensure service continuity.

Protection from Vulnerabilities including Malware

- The department/organisation shall ensure from the services provider for all security control measures to address the latest vulnerabilities and insecurities that could bring the system down or result in information disclosure or destruction.

Backup

- The department/organisation shall maintain Backup register that contains complete records of the backup copies such as Site location, Device type, Name, Backup type, frequency, Backup location, date etc.
- Backup kept any external media shall be encrypted;

Logging and Monitoring

- Regular monitoring of the audit log shall take place and results shall be recorded for necessary analysis as and when required to prevent unauthorized use of information systems

- Audit logs recording user activities, exceptions, and information security events shall be produced and kept until the next audit is performed to assist in future investigations and access control monitoring;

Technical Vulnerability Management

- Vulnerability assessments including penetration testing and application security testing shall be performed on an on-going basis
- Insecure remote access to database, application server shall be disabled
- Default configuration must be modified as per the organization need.
- Secure configuration must be used as an example SSHv2 instead of Telnet, SNMP vesion3 instead of version1&2, IPsec vpn instead of GRE tunnel.

Communication Security

- All connections initiated from outside to the department/organisation networks and vice versa shall be routed and controlled through firewalls positioned at the network boundaries
- The access rules of firewalls shall be maintained only by respective personnel responsible for firewall administration
- Procedures shall be documented to ensure controls (such as technical controls, contracts/agreements) implemented to exchange business information with stakeholders, third parties and within the department/organisation
- Technical controls shall be designed and implemented to prevent unauthorized interception, modification and interruption of the information transmitted through email system, all messages generated by email shall be considered the property of the department/organisation.
- Confidentiality or non-disclosure agreements shall address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements shall be applicable to external parties or employees of the department/organisation.

System Acquisition, Development & Maintenance

- All new information systems or services that are acquired, developed or enhanced shall undergo security assessment, to ensure that security controls are incorporated.
- Prior to deployment, all publicly available systems i.e. website, web services, mobile apps etc. shall be tested and it shall be ensured that the identified vulnerabilities are fixed prior to publishing any information in such systems.
- Information involved in application services transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay via SSL/TLS
- Secure development shall be followed to build up a secure service, architecture, software and system considering security of the development environment, security requirements in the design phase, security check points within the project milestones, security in version control and likewise.

- User Acceptance Testing (UAT) shall be conducted prior to the deployment of the systems in the production environment.

Supplier Relationships

- The department/organisation shall ensure the right to monitor, review and audit the OEM/supplier/vendor or any third-party providing service delivery.
- Agreements with third-parties involving accessing, processing and communicating of information shall cover all relevant security requirements.
- Description of the information to be provided or accessed and methods of providing or accessing the information shall be identified
- Audits shall be conducted at specified intervals to assess the compliance of third-parties with the agreed contracts and the clauses incorporated in the contracts

Information Security Incident Management

- Employees of the department/organisation and third-party vendors shall be made aware of procedures for reporting a security incident.
- Necessary procedures shall be put in place for detecting, reporting, responding and recording security incidents.

Information Security Aspect of Business Continuity Mgmt.

- A comprehensive Business Continuity Plan (BCP) that includes RTO (Recovery time objective) and RPO (Recovery Point Objective) shall be developed and implemented in order to maintain or restore business operations in the required time scales
- The department/organisation shall identify business requirements for the availability of information systems

Compliance

- Intellectual Property Rights (IPR) shall be included in all the contracts, and shall be implemented.
- The importance of privacy shall be communicated to all employees involved in the processing of Personally Identifiable Information (PII) and sensitive information.
- The data protection and privacy of PII against unauthorized access, transmission, publication, damage, use, modification, disclosure and impairment shall be ensured by implementing technical and administrative control.

Cryptography

- The key management for secure key generation, ownership, distribution, archival, storage and revocation shall be performed to protect the keys throughout their

lifecycle. The cryptographic keys shall be protected against unauthorized modification, substitution, unintended destruction and loss.

- Organization must manage Digital certificate throughout the life cycle for their application, they must ensure to renew the digital certificate before expiry date and install the same in live application.