Draft Policy for Information Security in offices Of Punjab Government

Government of Punjab

Department of Governance Reforms,
SCO 193-195, Sector-34A,
Chandigarh-160022

Date of Issue : …….

1.0 Purpose

This policy establishes rules, procedures and guidelines for persons accessing computer resources in order to ensure the confidentiality, integrity, and availability of data and resources.

2.0 Definitions

2.1. Confidentiality: Unauthorized access, reading or copying of information including data, program Code etc.

2.2. Integrity: Unauthorized manipulation of information including data, program code etc.

2.3. Availability: Unauthorized deletion of information including data, program code etc. or causing denial of service.

2.4. Information: An instance of an information type.

2.5. Information Resources: Information and related resources, such as personnel, equipment, funds, and information technology.

2.6. Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

2.7. Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

2.8. Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by

the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

2.9. Information Type: A specific category of information e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management, defined by a department/office, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

2.10. State offices: For the purpose of this policy 'state offices' include all the departments/boards/corporations/commissions of Government of Punjab.

3.0 Objective

3.1. To sensitize Punjab State departments, boards, corporations, commissions regarding importance and need for adequate corrective and preventive measures to be taken for information security in their respective offices.

3.2. To help state offices in formulating the mechanism for taking adequate measures in the area of Information security, such as access control, Confidentiality, data loss, data theft, Integrity, authentication etc.

3.3. To help state offices in laying down well defined procedures for safeguarding computer hardware, system software, application software, data, Information, documentation stored and transacted, in stand-alone computers or computer networks.

3.4. To suggest a mechanism for drawing up a plan for third party security audit.

3.5. To evolve a mechanism for coordinating with other central agency / agencies involved in Information security.

3.6. To suggest measures for obtaining International Security Standard Certifications such as ISO 27001 wherever applicable.

3.7. To provide guiding principles in the area of information security technology initiatives in the state of Punjab.

3.8. To facilitate state offices in incorporating Information Security guidelines in their Request for Proposal (RFP) documents to enable the vendors/contractors to follow the same during the design, development, installation, commissioning and operations of an IT, e-Gove applications/system for the respective state offices.

4.0 Information Security Principles

The state offices may follow following guiding principles for safeguarding "Information" in terms of confidentiality, integrity and availability in order to provide trusted services. These principles must be kept in mind to protect Information at Infrastructure, network and application level during operations and management of IT/e-gov application/systems.

4.1. All state offices may classify information as Confidential, Restricted for Internal use and for public use according to its appropriate level of confidentiality, integrity and availability. This may further be classified in accordance with IT Act 2000 and IT Act Amendment 2008 and/or other applicable relevant Legislative, regulatory and contractual requirements.

4.2. All the state offices shall document and implement adequate policies/procedures/system for handling the information by its employees in accordance with its classification level as defined in clause 4.1 of this policy.

4.3. All state offices may ensure that Information is both secure and available to those with a legitimate need for access and may be

protected against unauthorized access and processing in accordance with its classification level.

4.4. All state offices may ensure that Information is protected against loss or corruption.

With a view to implement Information security principles as defined in section 4.0 of this policy, it is recommended that all state offices may document and implement following procedures to secure information in their respective officials.

5.0 Incident Response

Incident response is an organized approach of identifying, addressing, managing and reporting the aftermath of a security breach or attack (also known as an incident).

5.1. All state offices may constitute an Incident Response Team to report, preliminary analyse any Information Security Incident and submit the recommendations to the Head of respective office for corrective and preventive measures to be taken to avoid further occurrence of similar incident(s).

Below are the few type of Incidents and response to same.

5.1.1. System Compromise:

Incident: System is compromised on account of virus attack.

Response: Compromised system after detection, should be immediately disconnected from the network. A genuine version of the operating system and all security-related software be reloaded, as well as user and system privileges shall be reviewed for modifications. The reloading takes place after evidence collection/disk imaging has taken place. Evidence collection/disk imaging shall be taken prior to any system changes to preserve the affected scenario.

5.1.2. Privileged Account Compromise:

Incident: The password of the system is leaked and system is used by unidentified person.

Response: All passwords on that system shall be immediately changed and any other systems utilizing that account. The system shall be checked thoroughly about the access of files.

6.0 Identification and Authentication

Identification is the process of recognizing a valid user's identity. Authentication is the process of verifying the claimed identity person, a process, or a system (e.g., an operations system or another network element) that accesses a network or its element to perform tasks. While implementing eGov/IT applications/Systems, all the state offices may implement adequate Identification and Authentication provisions in their eGov/IT system and its elements (network devices, Application software, System software, Computer etc.). The Identification and Authentication procedures to be implemented must include the following:

6.1. Procedure to validate and authorize functions or privileges of a person, a process, or a system (e.g., an operations system or another network element) by a secure means, within a reasonable amount of time, and without undue difficulty as per the global access control policy and at the application level.

6.2. The use of digital signatures, passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof for the authentication of user identity.

6.3. Limit of consecutive invalid authentication attempts by a user during a specified short time period. The application should automatically locks the account for a specified time interval, when the maximum number of unsuccessful attempts is exceeded.

6.4. The use of quality authentication secret ie session tokens shall be of adequate length, passwords shall be random in nature with validity (Refer 9.0 for password policy).

7.0 Password Security

All the state offices may document and implement adequate policies/procedures for password security of Infrastructure, Application, Systems, network elements etc. While implementing of such procedures, following must be taken into account:

7.1. Restrict use of blank passwords, dictionary words

7.2. Minimum length of password and use of alpha-numeric password.

7.3. Expiry of the password after specified time period (typically 30 days).

7.4. Restricting re-use of specified number (typically 3) of earlier used authentication secrets.

7.5. Restricting change of authentication secret in quick successions by specifying a minimum period (typically 1 day) after which the password can be changed.

7.6. Application Account Passwords shall not be granted access to any user until a deviation has been submitted and approved.

7.7. Application Account Password shall not be shared except with pre-determined approved users required to support the application.

7.8. Email account password shall be changed at regular interval (typically every 30 days).

7.9. Password Storage: If passwords are stored on the network in a file share, access to the file share shall be limited. The file or file system storing the password should be encrypted.

8.0 Virus attacks and Response

All state offices may document and implement adequate procedures in their respective offices to ensure a virus free environment. These procedures must include:

8.1. Device/Hardware: All devices capable of sending or receiving any virus shall run approved anti-virus software with up-to-date virus definition files at all times. Each device shall update virus info files at least once daily.

8.2. Data/Software: Any data/software being transmitted across the LAN/WAN is subject to scanning for harmful content by the anti-virus software suite.

8.3. User notification: All users from all department, board, commission & corporation shall be notified of the existence of significant virus threats and instructions for handling them.

8.4. Treatment of non-compliant devices: Any device connected to a network in violation of this virus security policy shall be disconnected from the network immediately. A list of devices not meeting the virus requirements shall be approved and kept up-to-date by each location.

9.0 Network Security

All the state offices shall document and implement adequate procedures to control and regulate the information flow within the system and between interconnected systems including the network boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers). Following guidelines may be followed while implementing such procudures:

9.1. Network Log-in Banner :The following warning banner shall be displayed on login screen of the computers:

"*W A R N I N G!! This is a restricted system for authorized users only. You are attempting to log into a private and secure device where all activities are monitored and logged. You are advised that if such monitoring reveals*

possible criminal activity, system personnel may provide the evidence of such information to law enforcement officials. W A R N I N G!!"

9.2. Device Passwords: All the internal and external network devices (routers, firewalls, access control servers, etc.) shall have unique passwords and access control mechanisms.

9.3. Prior approval for multi-user systems: Employees of all state offices may not establish electronic bulletin boards, local area networks, modem connections, or extranet connectivity to existing networks, VPN connections, wireless networks, or other multi-user systems for communicating information outside of network without specific approval from the Information Security Team.

9.4. Any type of documents pertaining to internal system IP addresses, configurations, and related system design information shall be restricted such that both systems and users outside department, board, commission & corporation internal network cannot access this information. All such documents are only shared on a strictly need to know basis.

9.5. Visitors Internet Connections: All visitors' network connection shall be approved through the deviation process and shall meet the internet connection security guidelines.

9.6. Third-Party Networks: Internal networks may only be connected to third party networks after the Information Security Team has determined that the combined system will be in compliance with the provisions of this Security Policy.

9.7. All systems accessible via the Internet shall be protected by a security appliance approved by the Information Security Team. The Internal network connected to an external organization shall be protected by a firewall.

9.8. Virtual Private Network: The establishment of a direct connection between department, board, commission & corporation systems and systems at

external organizations, via the Internet or any public network, is prohibited unless this connection has first been approved by the Information Security Team.

9.9. All internet connections attached to the department, board, commission & corporation trusted network shall be monitored by an Intrusion Detection/ Prevention System (IDS/IPS) approved by the Information Security Team.

9.10. All internet connections shall be directed through a content filter technology to protect internal network from adware, spyware, malware, and other vulnerabilities that exist through internet browsing.

9.11. Local Proxy Servers shall not bypass in any way the Internet content filtering solution and be approved through the deviation process.

9.12. No wireless networks, other than those approved by the Information Security team, are permitted.

9.13. Wireless Network Authentication: All computing devices shall be able to authenticate through encrypted means to access wireless networks. The Information Security Team shall approve each method of authentication. Prior to purchase of wireless equipment, you shall be sure it is capable of performing the required encryption services. If your wireless network does not meet this criterion you shall follow the Information Security Deviation Process. (Refer wi-fi policy of state for details).

10.0 Application Design Security

10.1. Access Control per Data Sensitivity: All production applications shall provide access control commensurate with functionality and data sensitivity.

10.2. Production applications shall provide adequate separation of duties control mechanisms commensurate with functionality and data sensitivity.

10.3. All production applications shall provide privacy in accordance with all corresponding government laws.

10.4. Applications shall provide adequate legal and business-function record retention. (Refer CII Policy of the State)

10.5. Applications shall be backed-up in such a manner that a full system rebuild could be accomplished using original distribution media and backup volumes.

10.6. Target systems that receive data from other applications shall apply equal or greater security than the data source application.

10.7. All production applications shall provide users with the ability to change their own passwords.

10.8. For all production applications that use application level security where a password is stored internally (in the application's database), the password shall be encrypted or protected.

10.9. Account IDs and/or passwords shall not be hard coded into application source code.

11.0 Application Development

11.1. All application development shall follow the approved application change process, inclusive of all required documentation incorporated into IT's Service Management processes.

11.2. Developers shall not promote their own code into production for sensitive functional areas in any circumstance exception being: line down and emergency implementation plan with roll back procedures

11.3. Application shall follow a review process for modification to existing code and new code prior to promotion into production.

11.4. Developers should not be able to execute any transaction in PRD except the exception noted above.

11.5. Source code shall be controlled and access restricted via an approved security solution (PVCS, VSS, etc.) handled on an individual basis.

11.6. Source code should never be distributed to any of customers or third party unless approved by the Information Security Team and a signed NDA.

12.0 Database Security

12.1. All production applications shall have a defined and documented security model which shall include user defined database roles, application roles (if necessary), user access models, and user access approval procedures.

12.2. All database and/or code modifications for any production database shall be promoted through an approval process by the usage of an approval panel consisting of database administrators, developers, and management.

12.3. All non-emergency production database modifications should be promoted through a development, test, and staging process prior to production. Emergency code promotion requires testing and management approval.

12.4. All database servers/database names shall follow a naming convention that clearly distinguishes development (DEV), testing (TEST), STAGING (STG) and production (PRD) environments.

12.5. All modifications including configuration and coding changes to production databases shall be tracked through a change management process. Documentation should include the time, purpose, modifier, etc.

12.6. Unique login requirement: Anyone logging into a database, shall log in using his or her own user account. No user shall log into a production database using the application account, another users account, an

application account, or as an Administrative or Services account. All user accounts access shall have prior management approval.

12.7. Except for application, direct database access to a non-reporting production database is prohibited through any modification tools. Developers shall not have direct write access to any production database. Troubleshooting access can be provided on an as needed basis through an established approval process.

12.8. No Direct Data Access to Global Data Sources: Administrator shall never grant Users access to the data directly, they shall go through an application interface.

13.0 System Patches

13.1. All state offices may document and implement adequate procedures to be implemented security patches for applications, development tools, and operating systems shall be tested and applied in accordance with their guidelines by their Infrastructure team.

13.2. Security Patches Installation: All systems in the network shall be patched regularly with all required Security patches rolled out through the Incident/Hot Fix Process.

13.3. Non-Compliant Patched Systems: Computers unable to meet compliancy objectives will be documented through the appropriate security deviation process.

14.0 Application Account Security

14.1. Application Administrator Access: Application administrators shall be restricted from changing their own access rights. Manager approval is required to promote a user to application administrator. The approving authority cannot be the one that executes the change.

14.2. User access privileges should be assigned based on current job-role and updated as job function requirements and user status change. This includes termination.

14.3. Protected Group Modification: Any change of membership to the system level privilege groups requires a workflow approval from competent authority.

15.0 Auditing and Logging

All departments, boards, corporations and commissions of Government of Punjab should implement Logging mechanism to record pre-defined events, activities to facilitate time-correlated audit trail. The Information system should produce audit records that contain sufficient information to establish what events occurred and when, the sources of the events, and the outcomes of the events. The audit and logging system shall have provision:

15.1. To generate audit records in commonly used standard formats.

15.2. To centrally manage the content of log records.

15.3. Capability of inclusion of additional, more detailed information in the audit records for audit events identified by type, location or subject.

15.4. Of Access control system to protect log records from alterations like editing, and deletion.

16.0 IT Security Audit

Department of Governance Reforms recommends to all state offices to document and implement procedures for periodic Information Security audits for all the critical IT applications, assets as the case may be. For this purpose following guidelines may be followed:

16.1. All critical IT applications and assets, should be audited by a certified third party IT Security auditing agency.

16.2. A list of the applications and assets to be considered for audit should be drawn up by periodically.

16.3. The nodal office of the state office will be responsible for ensuring that all the important IT applications / assets under his control are covered by a plan for IT Security audit.

16.4. Getting the IT Security audit conducted will be the responsibility of the designated nodal officer of the state office and application owner.

17.0 Information Security Cell

17.1. Department of Governance Reforms shall setup Information Security Cell (ISC) in Punjab State e-Governance Society (PSeGS) which shall be responsible for studying threats, risks, vulnerabilities and their solution, providing security bulletins and teaching and enforcing activities related to Information Security and auditing the implementation of Information security principles in the office(s) of Punjab Government.

17.2. Information Security Cell will facilitate the process of creating, documenting, reviewing, updating and implementing security procedures/policies in all the state offices.

17.3. Department of Governance Reforms will recruit Information security professionals or engage professional consultants for assisting state government officials in formulating, implementing and auditing Information security procedures/policies.

17.4. Department of Governance Reforms will facilitate to conduct appropriate training in the area of Information Security for Government officers/officials on regular basis.

18.0 Interpretation & Modification of Policy

18.1. This Policy shall be valid for three years from the date of issuance of this policy.

18.2. Department of Governance Reforms reserves the right to bring any amendment, addendum, modification, revision etc. to this policy. Changes in the regulatory framework, technology, as well as market and technological advances may require revisions to this policy to keep the requirements and guidelines updated with the prevailing environment.

19.0 Effective Date:

19.1. This policy will be applicable with immediate effect.

20.0 Approval

20.1. This policy has been approved by the Council of Ministers as conveyed by the Department of General Administration Punjab vide their letter number < >, dated < >.

****

References:

1. National Cyber Security Policy 2013

2. Information Security Management System (ISMS) – STQC

3. e-Governance Security Assurance Framework - e-Governance Standards

