Enterprise Information Security Policy
Personnel Security

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for establishing appropriate personnel security controls to ensure that safeguards are applied for access and use of Information Technology (IT) Resources and data. Such safeguards include, but are not limited to, conducting appropriate personnel screening and background checks, conducting security awareness training, and executing non-disclosure agreements for individuals needing access to sensitive, confidential, or regulated information. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

It is the policy of the State of Illinois that access to State of Illinois IT Resources will be limited to only those persons who have been appropriately screened and authorized. Agency will ensure that individuals occupying positions of responsibility (including third-party providers) (i) meet established security criteria for those positions, (ii) protect IT Resources during and after personnel actions, and (iii) comply with state and federal laws, rules, and regulations.

2. GOAL

The goals of this Policy are to (i) mitigate the risk of personnel intentionally or inadvertently exploiting their legitimate access to information assets for unauthorized purposes, which may have negative impacts, and (ii) secure the confidentiality, integrity, and availability of information.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Information Security - Position Risk Designation

4.1.1 Agencies shall establish and maintain standards to ensure appropriate levels of personnel screening for all personnel accessing State of Illinois IT Resources. Standards will include:

- defined risk designation levels based on the sensitivity of the information that the individual is required to access for legitimate position responsibilities;
- screening criteria for each risk designation level; and
- periodic reviews and updates to position risk designations.

4.2 Personnel Screening

4.2.1 Individuals will be screened by Agencies prior to being granted access to the applicable information and system(s).

4.2.2 Personnel will be screened by Agencies (i) as part of the establishment of access to the State of Illinois network, (ii) when a change in policies, laws, rules, and/or regulations warrants additional or renewed screening, and (iii) when changes in position and/or responsibilities require access to information that would place the individual into a different risk designation.

4.2.3 Personnel requesting access to State of Illinois IT Resources must comply with the submission of required documentation.

4.3 Personnel Termination

4.3.1 It is the responsibility of Agencies to notify DoIT of personnel employment terminations without delay following the employment termination.

4.3.2 Exit interviews will be conducted by the individual's Agency to review the terms of any applicable non-disclosure agreements and to ensure that the individual separating is informed that State of Illinois confidential and sensitive information shall not be removed, retained, or communicated to third parties.

4.3.3 Agency will terminate, revoke, or render inoperable the terminated individual's access credentials.

4.3.4 Agency will ensure that all Information System devices and authentication devices or tools are obtained from the individual and either returned to DoIT or re-allocated to appropriate personnel.

4.3.5 Agency information and Information Systems formerly controlled by the terminated individual will be retained by Agency, as appropriate.

4.4 Personnel Transfer

4.4.1 Agency will review and confirm ongoing operational need for current logical and physical access authorizations to Information Systems/facilities when individuals are reassigned or transferred to other positions within the Agency.

4.4.2 Agencies must notify DoIT when an individual is transferring to another state Agency.

4.4.3 DoIT will make appropriate changes to required access following the transfer or when DoIT is advised of the transfer.

4.5 Access Agreements

4.5.1 Agencies must develop and document access agreements for their Information Systems in compliance with established policies, laws, rules, and regulations.

4.5.2 Agencies must review and update access agreements in line with applicable laws, rules, and regulations.

4.5.3 Agencies must ensure that individuals requiring access to information and Information Systems:
(1) sign appropriate access agreements prior to being granted access; and

(2) re-sign said agreements to maintain access to Information Systems when access agreements have been materially updated or when access requirements change.

4.6 Third-Party Personnel Security

4.6.1 Third-party providers and third-party personnel must comply with this Policy and all other information security policies.

4.6.2 It is the responsibility of third-party providers to submit any and all documentation as identified in applicable standards as assurance of compliance with this Policy.

4.6.3 Third-party providers must notify the employing Agency of any transfers or terminations of personnel who possess Agency credentials and/or badges, or who have Information System privileges.

4.6.4 DoIT will periodically review compliance regarding third-party personnel security. Third-party providers must provide DoIT with requested information to help ensure compliance with this Policy.

4.7 Denial and/or Termination of Access

DoIT's Office of the Chief Information Security Officer and/or other Agency-designated senior management may deny or terminate access to State of Illinois information and systems by personnel who have not been appropriately screened in accordance with this Policy and/or who are deemed ineligible for information access based on personnel screening criteria.

4.7.1 Should the DoIT Chief Information Security Officer (CISO) or authorized delegate determine that denial or termination of access is warranted, the CISO will notify the impacted Agency-designated senior management of the intent to deny or terminate access. The notification to Agency-designated senior management shall be in writing. Electronic mail may be utilized to provide the notification.

4.7.2 In the case of an imminent threat as determined by the CISO or authorized delegate, termination of access may take place immediately.

4.7.3 The Agency-designated senior management may request an exception to the access denial/termination decision. The exception request shall be in writing to the CISO and/or other Agency-designated senior management. Electronic mail may be utilized to request the exception.

4.8 Information Security Training

4.8.1 Employees seeking or retaining access to State of Illinois IT Resources must undergo information security awareness training in compliance with applicable laws, rules, and regulations.

4.8.2 Information security training must be completed within 30 days of acquiring access to State of Illinois IT Resources.

4.8.3 Employees must undergo information security training on an annual basis between January 1 and December 31 of each year.

4.8.4 DoIT is responsible for providing information security training in compliance with State of Illinois statute 20 ILCS 450/25 and any adopted rules and standards.

4.8.5 Agencies are responsible for ensuring Employee compliance with this Policy.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security establishes supplemental policies, standards, procedures, and guidelines and may designate responsibility to specific personnel. To the extent necessary, each Client Agency and/or DoIT Division must establish procedures in order to achieve Policy compliance. It is the responsibility of all authorized Employees of IT Resources to understand and adhere to this Policy.

Failure to comply with this Policy may result in the Chief Information Security Officer temporarily discontinuing or suspending the operation of the Information System, solution, and/or resource until such compliance is established as deemed solely by the Chief Information Security Officer. Failure to comply with this Policy could also result in the loss of access to State of Illinois IT Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.