State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Security Planning

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) will ensure the protection of State of Illinois information technology (IT) assets from unauthorized access, modification, disclosure, and destruction. This Policy establishes the minimum-security requirements to ensure a consistent security baseline. This Policy also provides direction to coordinate information security program planning activities to effectively manage risk and to protect the State of Illinois information assets. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to ensure that planning activities are accomplished to provide protection to the confidentiality, integrity, and availability of State of Illinois information assets.

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" shall include both DoIT and Client Agencies.

4.1 System Security Plan

4.1.1 Agency shall develop a security plan for the Information System that:

- is consistent with the enterprise architecture;
- explicitly defines the authorization boundary for the system;
- describes the operational context of the Information System in terms of missions and business processes;
- provides the security categorization of the Information System including supporting rationale;
- describes the operational environment for the Information System and relationships with or connections to other Information Systems;
- provides an overview of the security requirements for the system;
- identifies any relevant overlays, if applicable;
- describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
- is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

4.1.2 Agency shall distribute copies of the security plan and communicate subsequent changes to the plan to the State of Illinois Chief Information Security Officer.

4.1.3 Agency shall review the security plan for the Information Systems at a defined frequency based on risk.

4.1.4 Agency shall update the plan to address changes to:

- the Information System;
- environment of operation;
- problems identified during plan implementation; and
- security control assessments.

4.1.5 Agency shall utilize Least Privilege protocol to protect the security plan from unauthorized disclosure and modification.

4.2 Information Security Architecture

4.2.1 Agency shall develop an Information Security architecture plan that:

- describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of information;
- describes how the information security architecture is integrated into and supports the enterprise architecture; and
- describes any information security assumptions about, and dependencies on, external services.

4.2.2 Agency shall review and update the information security architecture plan on a defined frequency to reflect updates in the enterprise architecture.

4.2.3 Agency shall ensure that information security architecture changes are reflected in the security plan and procurements.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security establishes supplemental policies, standards, procedures, and guidelines and designates 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 Employees 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.