1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes the requirements for security assessment and authorization to ensure that necessary security controls are integrated into systems and processes. Security assessments allow management to assess existing risk and ensure that security and privacy controls have been implemented. 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 establish a security assessment and authorization capability throughout State of Illinois agencies, boards and commissions. Specifically, this Policy will support the implementation of security best practices.

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 Security Assessments

4.1.1. Agency shall develop a security assessment plan that describes the scope of the assessment, including:

- security and privacy controls and control enhancements under assessment;
- assessment procedures to be used to determine control effectiveness; and
- assessment environment, assessment team, and assessment roles and responsibilities.

4.1.2. Agency shall assess the security controls in the Information System and its environment of operation within an established timeframe to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

4.1.3. Agency shall produce a security assessment report that documents the results of the assessment.

4.1.4. Agency shall formally provide the results of the security control assessment to Agency senior management.

4.2. Information System Connections

This control applies to dedicated connections between Information Systems and does not apply to transitory, user-controlled connections such as email and website browsing.

4.2.1. Connections from the Information System to other Information Systems outside of the authorization boundary must be authorized by Agency senior management through the use of Interconnection Security Agreements (ISAs).

- If the connecting systems have the same Authorizing Official, an ISA is not required.

Rather, the interface characteristics between the connecting Information Systems must be described in the security plans for the respective systems. Instead of developing an ISA, Agencies may choose to incorporate this information into a formal contract.

- If the connecting systems have different Authorizing Officials, but the Authorizing Officials are in the same Agency, DoIT shall determine whether an ISA is required, or alternatively, the interface characteristics between the connecting Information Systems must be described in the security plans for the respective systems.

4.2.2. For every Sensitive Agency Information System that shares data with non-State of Illinois entities, the Agency shall require or shall specify via written agreement (an ISA) that its service provider comply with the following requirements:

- The System Owner, in consultation with the Business Owner, shall document Information Systems with which data is shared. This documentation must include:
  i. the types of shared data;
  ii. the direction(s) of data flow; and
  iii. contact information for the Agency that owns the Information System with which data is shared, including the System Owner, the Information System Security Officer (ISSO), or equivalent, and the System Administrator.
- The System Owners of interconnected systems must inform one another of connections with other systems.
- The ISA shall specify if and how the shared data will be stored on each Information System.
- The ISA shall specify that System Owners of the Information Systems that share data acknowledge and agree to abide by any legal and/or regulatory requirements.
- The ISA shall specify each Business Owner's authority to approve access to the shared data.
- The System Owners shall approve and enforce the written agreement.
- Risks that may be introduced when Information Systems are connected to other systems with different security requirements and security controls must be carefully considered. The Authorizing Official shall determine the risk associated with each connection and the appropriate controls to be employed.

4.3. Security Authorization

Security authorization is the official management decision, conveyed through the authorization decision document of an Information System, explicitly accepting the risk to Agency operations.

4.3.1. For each Information System, the ISO or equivalent designee shall:

- assign a State of Illinois employee in an existing senior-level executive or managerial position to serve as the Authorizing Official;
- ensure that the Authorizing Official authorizes the Information System for processing before commencing operations; and
- update the security authorization based on a defined frequency.

4.4. Continuous Monitoring

A continuous monitoring program maintains the security authorization of an Information System.

4.4.1. The ISO or equivalent designee shall establish a continuous monitoring strategy and implement a continuous monitoring program that includes:

- a configuration management process for the Information System and its components;
- a determination of the security impact of changes to the Information System and environment of operation;
- ongoing security control assessments in accordance with the Agency's continuous monitoring strategy; and
- reporting the security state of the Information System to appropriate Agency officials.

4.4.2. The implementation of a continuous monitoring program results in ongoing updates to the security plan.

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 Information Technology (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.