State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Privacy: Accountability, Audit, and Risk Management

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) will protect the confidentiality of Personally Identifiable Information (PII) by establishing minimum baseline controls that reduce the risk of adverse events associated with privacy and confidentiality. 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 integrate the privacy, accountability, audit, and risk management requirements as part of data collection to mitigate risk and effectively manage 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" shall include both DoIT and Client Agencies.

4.1. Governance & Privacy Program

Agency shall:

- appoint individuals accountable for developing, implementing, and maintaining an Agency-wide governance and privacy program to ensure compliance with applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII.
- monitor privacy laws and Agency policies for changes that affect the privacy program.
- allocate sufficient resources to implement and operate the Agency-wide privacy program.
- develop a strategic privacy plan for implementing applicable privacy controls, policies, and procedures.
- develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, Information Systems, or technologies involving PII.
- update privacy plan, policies, and procedures on a defined frequency.

4.2. Privacy Impact and Risk Assessment

4.2.1. Agency shall develop and implement a privacy risk management process that assesses privacy risk for the collection, sharing, storing, transmitting, use, and disposal of PII.

4.2.2. Agency shall conduct Privacy Impact Assessments (PIAs) for Information Systems, programs, or other activities that pose a privacy risk in accordance with applicable law or respective Agencies' policies and procedures.

4.3. Privacy Requirements for Contractors And Service Providers

4.3.1. Agency shall include privacy requirements within contractual agreements for contractors and service providers.

4.4. Privacy Monitoring and Auditing

4.4.1. Agency shall monitor and audit privacy controls and internal privacy policies to ensure effective implementation.

4.5. Privacy Awareness and Training

4.5.1. Agency shall develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that Employees understand privacy responsibilities and procedures.

4.5.2. Agency shall administer basic privacy training annually.

4.5.3. Agency shall administer additional role-based training as required by federal, state, and Agency guidelines.

4.5.4. Agency shall ensure that Employees certify (manually or electronically) acceptance of responsibilities for privacy requirements.

4.6. Privacy Reporting

4.6.1. Agency shall develop, disseminate, and update reports to senior management and other Employees with responsibility for monitoring privacy program progress and compliance to demonstrate accountability with specific statutory and regulatory privacy program mandates.

4.7. Privacy-Enhanced System Design and Development

4.7.1. Agency shall design Information Systems to support privacy by automating privacy controls.

4.8. Accounting of Disclosures

4.8.1. Agency shall keep an accurate accounting of disclosures of information held in each system of records under its control, including:

- date, nature, and purpose of each disclosure of a record; and
- name and address of the person or Agency to which the disclosure was made.

4.8.2. Agency shall retain the accounting of disclosures according to defined retention requirements.

4.8.3. Agency shall make the accounting of disclosures available to the person named in the record upon request.

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.