State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Privacy: Security

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes appropriate and effective privacy security controls to protect, limit, or contain the impact of any incident involving a breach of Personally Identifiable Information (PII). Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

This Policy protects and ensures the proper handling of PII and provides effective responses to privacy incidents and breaches.

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 Inventory of Personally Identifiable Information (PII)

4.1.1 Agency shall establish, maintain, and update, on a defined frequency, an inventory that contains a listing of all programs and Information Systems identified as collecting, using, maintaining, or sharing PII.

4.1.2 Agency shall provide updates of the PII inventory to its Agency Chief Information Officer or information security official to support the establishment of information security requirements for all new or modified Information Systems containing PII.

4.2 Privacy Incident Response

4.2.1 Agency shall develop and implement a Privacy Incident Response Plan.

4.2.2 Agency shall provide an organized and effective response to privacy incidents and breaches in accordance with the Privacy Incident Response 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.

Revision history and approvals are reflected in ServiceNow.