Enterprise Information Security Policy
Privacy: Individual Participation and Redress

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) will protect the integrity of the Personally Identifiable Information (PII) it collects by obtaining informed consent, providing individuals with access to their own PII, and providing individuals a means for correcting the accuracy of their PII. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

This Policy addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By implementing this Policy, the State will provide individuals with a means to access their PII to have their PII corrected or amended, as appropriate. In turn, this Policy will lead to enhanced public confidence in the State's decisions related to collecting and using PII.

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 Consent

4.1.1 Agency shall provide the appropriate means for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

4.1.2 Agency shall provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

4.1.3 Agency shall obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

4.1.4 Agency shall ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the Agency collected the PII.

4.2 Individual Access

4.2.1 Agency shall provide individuals the ability to access their PII maintained on the appropriate system(s) of records.

4.2.2 Agency shall publish rules and regulations governing how individuals may request access to records maintained by Agency, in accordance with applicable laws and regulations.

4.2.3 Agency shall adhere to the applicable Agency privacy policies and applicable federal and state guidelines for the proper processing of privacy-related requests.

4.3 Redress

4.3.1 Agency shall provide a process for individuals to have inaccurate PII maintained by the Agency corrected or amended, as appropriate.

4.3.2 Agency shall establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners, and, where feasible and appropriate, Agency shall notify affected individuals that their information has been corrected or amended.

4.4 Complaint Management

4.4.1 Agency shall implement a process for receiving and responding to complaints, concerns, or questions from individuals about the Agency's privacy practices.

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.