State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy

Privacy: Data Quality and Integrity Policy

1. **OVERVIEW**

The State of Illinois Department of Innovation & Technology (DoIT) strives to enhance public confidence that any Personally Identifiable Information (PII) collected and maintained by the State of Illinois and its agencies, boards, and commissions is accurate, relevant, timely, and complete for the purpose for which the information is to be used. 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 maximize the quality, value, objectivity, and integrity of PII that the State of Illinois and its agencies, boards, and commissions collect.

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 Data Quality

- 4.1.1 Agency shall confirm, to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information.
- 4.1.2 Agency shall collect PII directly from the individual to the greatest extent practicable.
- 4.1.3 Agency shall check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems on a defined frequency.
- 4.1.4 Agency shall issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

4.2 Data Integrity

- 4.2.1 Agency shall document processes to ensure the integrity of PII through existing security controls.
- 4.2.2 Agency's Legal Office shall review and approve Computer Matching Agreements.

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.