State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy

Audit and Accountability Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) establishes this Enterprise Audit and Accountability Policy for managing risks from inadequate event logging and transaction monitoring. This Policy helps to identify accidental damage, disruption, physical tampering, eavesdropping, and other potential incidents and ensures the confidentiality, integrity, and availability of Information Systems and data within critical information technology (IT) assets. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

This Policy establishes an audit and accountability capability throughout DoIT and other State of Illinois agencies, boards, and commissions and their business units to implement security best practices for events, transaction logging, and retention of audit evidence.

3. SCOPE

This Policy applies to Users 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 Audit Events

4.1.1 Agency shall develop a standard that defines which security events to audit and the frequency of each audit. Agency shall review the list of events based on a defined frequency.

4.1.2 Agency shall determine auditable events in coordination with other entities requiring audit-related information.

4.1.3 Agency shall provide an explanation as to how audit events support investigations of security incidents when applicable.

4.1.4 Agency shall determine which events should be audited within the Information System.

4.2 Content of Audit Records

4.2.1 Audit records shall contain the following information:

- What type of event occurred
- When the event occurred
- Where the event occurred
- Source of the event
- Outcome of the event
- Identity of any individuals associated with the event

4.3 Audit Storage Capacity

4.3.1 DoIT shall allocate an adequate amount of storage capacity to ensure audit records can be retained for the required audit retention period.

4.4 Response to Audit Processing Failures

4.4.1 DoIT shall alert designated personnel when there is an audit processing failure.

4.4.2 DoIT shall create standards to define additional actions to follow in the event of an audit processing failure.

4.5 Audit Review, Analysis, and Reporting

4.5.1 DoIT shall review and analyze Information System audit records for indications of unusual activity related to potential unauthorized access.

4.5.2 DoIT shall report findings to designated personnel.

4.6 Audit Reduction and Report Generation

4.6.1 Agency shall employ audit reduction and reporting capability that supports on-demand audit review, analysis and reporting, and after-the-fact investigations of security incidents.

4.6.2 Agency shall not alter original content and time marking of audit records.

4.7 Time Stamps

4.7.1 State of Illinois Information Systems shall use internal Information System clocks to generate time stamps for audit records.

4.7.2 State of Illinois Information Systems shall record time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and shall synchronize internal Information System clocks to an enterprise-wide authoritative time source.

4.8 Protection of Audit Information

4.8.1 Agencies shall protect audit information and audit tools from unauthorized access, modification, and deletion.

4.9 Audit Record Retention

4.9.1 Agencies shall retain audit records to provide support for security incident investigations and to meet regulatory and Agency-specified requirements.

4.10 Audit Generation

4.10.1 The Information System(s) of DoIT and/or its Client Agencies shall provide audit record generation capability for all suitable events that are defined in this Policy or in the associated implementation standards and procedures.

4.10.2 Agencies shall designate personnel to select which events are to be audited by specific components of the Information System.

4.10.3 The Information System(s) of DoIT and/or its Client Agencies shall generate audit records for events defined by regulatory or Agency-specified requirements.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate 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 Users 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 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.