State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Information Security Incident Management

1. OVERVIEW

The ever-increasing number and diversity of cybersecurity-related attacks, as well as the State of Illinois' growing reliance on information and Information Systems for critical functions and services, requires a robust Information Security Incident response capability. While attacks from myriad threat sources place the State at risk, Information Security Incidents can also be caused by human error, lost or stolen equipment, environmental conditions, or other factors. Effective Information Security Incident Management capabilities must be in place to address any type of Information Security Incident that can significantly affect the State's ability to operate or that may cause damage.

This Policy defines management intent, expectations, and direction for the establishment of an Information Security Incident Management capability. 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 control the impact of State of Illinois Information Security Incidents within acceptable levels.

3. SCOPE

This Policy applies to Employees of the State of Illinois Department of Innovation & Technology (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. POLICY

DoIT will develop and maintain an Information Security Incident Management capability that:

- detects incidents quickly;
- diagnoses incidents accurately;
- manages incidents properly;
- completes timely and appropriate notifications;
- contains and minimizes damage of incidents;
- restores services affected by incidents;
- determines root causes of incidents;
- implements improvements to prevent recurrence; and
- appropriately documents incidents.

5. DEFINITIONS

5.1 Information Security Incident: A violation or imminent threat of a violation of information security policies, acceptable use policies, or standard security practices. The definition of an Information Security Incident includes but is not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data;
- an unwanted disruption or denial of service;
- a discovery of network intrusions including bot-nets;
- malware events;
- the unauthorized use of a system for the processing or storage of data;
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent;
- an unplanned, unauthorized, or unexpected change to security baselines, including an unauthorized change to security controls, technologies, or processes;
- the inappropriate release of personally identifiable or other confidential information;
- a theft or loss of information technology (IT) equipment that could contain non-public information; and
- a violation of information security policies.

5.2 Information Security Incident Management: The capability to effectively manage Information Security Incidents with the objective of minimizing impacts and maintaining or restoring normal operations.

5.3 Information Security Incident Response Plan: A predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against State of Illinois Information Systems.

6. 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.

6.1 Information Security Incident Response Training

6.1.1 Information Security Incident response training will be provided to Employees by DoIT on an annual basis.

6.1.2 Information Security Incident response Employees will be trained regarding their specific roles and responsibilities. Incident response Employee training will be conducted by DoIT on at least an annual basis to address any changes to the Information Security Incident Response Plan and to ensure currency of training.

6.2 Information Security Incident Handling

6.2.1 An Information Security Incident handling capability will be developed and maintained by DoIT that includes preparation, detection and analysis, containment, eradication, and recovery processes.

6.2.2 Agency shall coordinate incident handling activities with contingency planning activities.

6.2.3 DoIT shall incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing.

6.3 Information Security Incident Monitoring

6.3.1 Agency shall document and track Information Security Incidents.

6.4 Information Security Incident Reporting

6.4.1 All Employees, contractors, and third-party providers of State of Illinois shall report any and all Information Security Incidents to the DoIT Division of Information Security.

6.4.2 Information Security Incidents shall be reported to the DoIT Division of Information Security without delay, but no later than 24 hours following the discovery of an Information Security Incident.

6.4.3 The DoIT Division of Information Security shall work collaboratively with Employees of impacted or involved agencies, boards, and commissions to help ensure the appropriate reporting of Information Security Incidents to the Governor's Office, the General Assembly, the Attorney General, and/or other entities as required by policies, regulations, or laws.

6.4.4 The DoIT Division of Information Security shall provide guidance and input to executive management of agencies, boards, and commissions regarding potential reporting of Information Security Incidents to law enforcement.

6.4.5 The DoIT Division of Information Security may share information regarding Information Security Incidents with the Illinois State Police Statewide Terrorism and Intelligence Center (STIC), Multi-State Information and Analysis Center (MS-ISAC), and other trusted partners to help resolve, mitigate, or reduce the impact of cyber events on the State or the nation. External information sharing will not include Agency-specific information without the authorization of Agency executive management.

6.5 Information Security Incident Response

6.5.1 The DoIT Division of Information Security shall lead, manage, and coordinate the response to all Information Security Incidents. Information Security Incident responses will be conducted collaboratively with DoIT Divisions and the appropriate Employees from the impacted or involved agencies, boards, or commissions.

6.5.2 The DoIT Division of Information Security shall provide Information Security Incident response support resources, guidance, advice, and assistance to agencies, boards, and commissions to help ensure the effective handling and reporting of Information Security Incidents.

6.5.3 Third-party providers of Information Systems will provide Information Security Incident response cooperation and assistance relating to any Information Security Incidents that involve Information Systems provided by the third-party entity.

6.6 Information Security Incident Response Plan

6.6.1 The DoIT Division of Information Security shall develop and maintain an Information Security Incident Response Plan, subordinate plans, policies, procedures, and guidelines that:

- provide the State of Illinois with a roadmap for implementing its incident response capability;
- describe the structure and organization of the incident response capability;
- provide a high-level approach to the Agency's incident response capability;
- meet the unique requirements for the State of Illinois;
- define reportable incidents;
- provide metrics for measuring the incident response capability within the State of Illinois;
- define the resources and management support needed to effectively maintain and mature an incident response capability; and
- are reviewed and approved by the Chief Information Security Officer.

6.6.2 Third-party providers of State of Illinois Information Systems will develop and maintain as applicable information security incident response plans that meet or exceed the requirements defined in this Policy.

6.6.3 The Information Security Incident Response Plan and subordinate plans shall be protected from unauthorized public disclosure and modification.

6.6.4 The Information Security Incident Response Plan and subordinate plans shall be reviewed on a defined frequency by DoIT. The plans shall be updated by Agencies as appropriate to address system changes or problems encountered during plan implementation, execution, or testing.

6.6.5 Changes to the Information Security Incident Response Plan and subordinate plans shall be communicated to incident response Employee by designated DoIT staff.

7. 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 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 IT Resources and/or discipline, up to and including discharge.

8. 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

9. REVISION HISTORY

Original Effective Date	
Last Review Date	
Revised Date	

10. APPROVALS AND MANAGEMENT COMMITMENT

Effective upon latest signature below.

_____ Date: _____
DoIT Acting Secretary, Kirk Lonbom

_____ Date: _____
Chief Information Security Officer, Chris Hill

_____ Date: _____
DoIT General Counsel, Michael Delcomyn

(3) Payment Card Data Protection
(4) Protected Health Information Security

9. REVISION HISTORY

Original Effective Date	
Last Review Date	
Revised Date	

10. APPROVALS AND MANAGEMENT COMMITMENT

Effective upon latest signature below.

DoIT Acting Secretary, Kirk Lonbom — Date: 10/8/18

Chief Information Security Officer, Chris Hill — Date: 9/21/18

DoIT General Counsel, Michael Delcomyn — Date: 10/15/18