Enterprise Information Security Policy
Contingency Planning Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) Contingency Planning Policy ensures that Information Systems that are determined to be critical and essential to DoIT and Client Agencies' missions have recovery objectives defined, documented, and tested in the case of a catastrophic failure. 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 reduce the security risks and establish enterprise contingency planning measures and procedures. Contingency planning helps DoIT execute a coherent, organized, planned, and strategic response to Information System emergencies and other disruptive Information System events.

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 Contingency Planning

4.1.1 Information System contingency plans shall:

- 4.1.1.1 identify essential missions and business functions and associated contingency requirements.
- 4.1.1.2 provide recovery objectives and restoration priorities.
- 4.1.1.3 address contingency roles, responsibilities, and contact information of assigned individuals, as well as delegations of authority, orders of succession, and notification procedures.
- 4.1.1.4 address maintaining essential missions and business functions despite an Information System disruption, compromise, or failure.
- 4.1.1.5 address eventual, full Information System restoration without deterioration of the security safeguards originally planned and implemented.
- 4.1.1.6 be reviewed and approved by designated officials within DoIT.

4.1.2 Agency shall distribute copies of the contingency plan to key contingency personnel.

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

4.1.4 Agency shall review the contingency plan for the Information System at a DoIT-defined frequency.

4.1.5 Agency shall update the contingency plan to address changes to the Information System or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

4.1.6 Agency shall communicate contingency plan changes to the key contingency personnel.
4.1.7 Agency shall protect the contingency plan from unauthorized disclosure and modification.

4.2 Contingency Training

4.2.1 Agency shall provide training for personnel in their contingency roles and responsibilities with respect to the Information System on a defined frequency, and Agency shall provide refresher training when changes occur.

4.3 Contingency Plan Testing

4.3.1 Information System contingency plans must be tested by the Client Agency with the assistance of DoIT resources on a defined frequency to determine the plan's effectiveness and the Agency's readiness to execute the plan.
4.3.2 The contingency plan test results must be reviewed, and issues must be noted and mitigated to an acceptable level, by the respective Client Agency's designated personnel to ensure the validity of the plan.

4.4 Alternate Storage Site

4.4.1 DoIT shall establish an alternate storage site, including necessary agreements to permit the storage and recovery of Information System backup information.
4.4.2 Agency shall ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

4.5 Alternate Processing Site

4.5.1 Agency shall establish an alternate processing site, including necessary agreements to permit the resumption of Information System operations for essential missions and business functions within a defined time period consistent with recovery time objectives when the primary processing capabilities are unavailable.
4.5.2 Agency shall ensure that equipment and supplies required to resume operations are available at the alternate site to support delivery to the site in time to support the defined time period for resumption.
4.5.3 Agency shall identify an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.
4.5.4 DoIT shall configure the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.
4.5.5 Agency shall ensure that the alternate processing site provides information security measures equivalent to that of the primary site.

4.6 Telecommunications Services

4.6.1 DoIT shall establish alternate telecommunications service plans, including necessary agreements to permit the resumption of Information System operations for essential missions and business functions within a defined time period when the primary telecommunications capabilities are unavailable.

4.7 Information System Backup

4.7.1 Agency shall conduct periodic backups of User information contained in the Information System within a defined frequency consistent with recovery time and recovery point objectives.

4.7.2 Agency shall conduct periodic backups of system-level information contained in the Information System in accordance with a defined frequency consistent with recovery time and recovery point objectives, including system-state information, operating system, application software, and licenses.

4.7.3 Agency shall conduct periodic backups of Information System documentation, including security-related documentation in accordance with a defined frequency consistent with recovery time and recovery point objectives.

4.7.4 Agency shall protect the confidentiality and integrity of backup information at the storage locations.

4.7.5 Agency shall test backup information within a defined frequency to verify media reliability and information integrity.

4.8 Information System Recovery and Reconstitution

4.8.1 Agency shall provide for the recovery and reconstitution of the Information System to a known state after a disruption, compromise, or failure.

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 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.