State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Supply Chain Risk Management Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) Supply Chain Risk Management Policy coordinates activities to strategically manage supply chain risk. 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 protect the State of Illinois information and Information Systems and to reduce supply chain risk through effective supply chain risk management practices in Illinois agencies, boards, and commissions.

3. SCOPE

This Policy applies to Users of DoIT and its Client Agencies.

4. REQUIREMENTS

DoIT and/or each of its Client Agencies, shall do the following, as outlined below, in connection with all Information Systems:

4.1 Supply Chain Risk Management Plan

4.1.1. DoIT and Client Agencies shall develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems, system components, or system services.

4.1.2. DoIT and Client Agencies shall review and update the supply chain risk management plan periodically as required, to address threat, organizational or environmental changes; and

4.1.3. DoIT and Client Agencies shall protect the supply chain risk management plan from unauthorized disclosure and modification.

4.2 Supply Chain Controls and Processes

4.2.1 DoIT and Client Agencies shall establish processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of system or system components in coordination with Agency personnel;

4.2.2 DoIT and Client Agencies shall employ controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events; and

4.2.3 DoIT and Client Agencies shall document the selected and implemented supply chain processes and controls in applicable security and privacy plans; supply chain risk management plans; and any other Agency-defined document.

4.3 Acquisition Strategies, Tools, And Methods

4.3.1 DoIT and Client Agencies shall employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

4.4 Supplier Assessments and Reviews

4.4.1 DoIT and Client Agencies shall assess and review the supply chain-related risks associated with third parties, the systems, systems component, and/or systems services they provide.

4.5 Inspection Of Systems or Components

4.5.1 DoIT shall develop a plan to inspect systems or system components upon delivery.

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 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 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 discipline, up to and including discharge. Client Agencies may submit to DoIT written requests for exceptions or waivers for any of the requirements of this Policy, which the Chief Information Security Officer may exercise discretion to allow or deny based on the best interests of the State.

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.