|  |  |  |
| --- | --- | --- |
| Policy #: | Title: | Effective Date: |
| x.xxx | Supply Chain Risk Management Policy | MM/DD/YY |

PURPOSE
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To ensure that supply chain risk management controls are implemented and in compliance with IT security policies, standards, and procedures.

POLICY
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This policy is applicable to all departments and users of [entity] resources and assets.

###### SUPPLY CHAIN RISK MANAGEMENT PLAN

IT Department shall:

1. 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 the following systems, system components or system services: systems used to access, process, store, or transmit CJI.
2. Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes.
3. Protect the supply chain risk management plan from unauthorized disclosure and modification.

###### SUPPLY CHAIN CONTROLS AND PROCESSES

IT Department shall:

1. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems, system components, or information system services which process, store, or transmit CJI in coordination with organization personnel with security responsibilities and supply chain risk management responsibilities.
2. Employ the following 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: security safeguards (e.g., avoiding the purchase of custom configurations to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations).
3. Document the selected and implemented supply chain processes and controls in the supply chain risk management plan.

###### ACQUISITION STRATEGIES, TOOLS, AND METHODS

IT Department shall:

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: use only suppliers who can provide attestations ~~of,~~ or demonstration of, compliance with state or federal standards.

###### SUPPLIER ASSESSMENTS AND REVIEWS

IT Department shall:

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide prior to entering into or upon any changes to an existing contractual agreement; upon the identification of evolving threats; changes in Federal laws, executive orders, directives, regulations; identification of emerging technology and information technology service delivery models; and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

###### NOTIFICATION AGREEMENTS

IT Department shall:

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises to systems used to access, process, store, or transmit CJI.

###### INSPECTION OF SYSTEMS OR COMPONENTS

IT Department shall:

Inspect the following systems or system components upon initial procurement and periodically as needed to detect tampering: systems used to access, process, store, or transmit CJI.

###### COMPONENT AUTHENTICITY

IT Department shall:

1. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system.
2. Report counterfeit system components to organization personnel with security responsibilities and external agencies as needed.

###### COMPONENT DISPOSAL

IT Department shall:

Dispose of CJI using the following techniques and methods: as described in MP.

COMPLIANCE

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Date Issued: | MM/DD/YYYY |
| Date Reviewed: | MM/DD/YYYY |