[Insert Company Name/Logo]	
Title: IT Supply Chain Business Environment & Risk Management	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team:**

Purpose

To ensure that our security policies will not contradict or hinder the organization's performance and/or place in the supply chain and critical infrastructure.

Scope

This policy applies to all employees and other members of the workforce (whether paid, volunteer or contractor) working in all facilities under the organization's ownership.

Policy

Our Security Officer will implement policies and procedures that align and coordinate with the organization's specific goals, missions, and purpose. This includes, but is not limited to, the organization's budget, mission statements, specific needs, etc. Our Security Officer will ensure that security policies will not contradict or hinder the organization's performance and/or place in the supply chain and critical infrastructure.

Procedures

ID.BE-1: The organization's role in the supply chain is identified and communicated.

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

1. Security officials will develop an organization-wide plan for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems and their components, and system services which includes:
    a. Potential security risks the supply chain would face such as:
        i. Security risk to organizational operations and assets.
        ii. Security risk to individuals. Potential security risk
        iii. Privacy risk to individuals results from processing personally identifiable information.
    b. Unambiguous expression of supplications risks tolerance.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

c. Acceptable supply chain risk mitigation strategies or controls.
d. Process for consistently evaluating and monitoring supply chain risk.

2. Security officials will Implement the supply chain risk management strategy consistently across the organization.
3. Security officials will review and update the supply chain risk management strategy as required, to address organizational changes.

ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.

ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

1. Security Officer will implement the following procedures to conduct a risk assessment which are not limited to:
    a. Assess the physical environment for potential damage to system components.
    b. Asset Identification and System Characterization.
    c. Vulnerability Identification and Threat Modeling.
    d. Risk Calculation and Mitigation.
    e. Provide the results of the risk assessment to [x]
2. Security Officer will implement the following procedures to minimize risks for the organization's critical infrastructure which are not limited to:
    a. Implement device related restrictions.
    b. Implement network-related restrictions.
    c. Implement safety-related restrictions.
    d. Implement runtime and uptime requirements.
    e. Minimize the opportunity for unauthorized physical access.

ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.

1. Security Officers will ensure that security and privacy considerations that are addressed throughout are explicitly related to the organization's mission.

Violations: Workforce members shall be responsible for reporting suspected or known information security concerns to the Security Officer as soon as discovered, with failure to do so resulting in appropriate sanctions**.**

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.