Insert Logo Here

Organization Name

Security Policy

System & Services Acquisition

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published SA Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68594235)

[2 Purpose 1](#_Toc68594236)

[3 Scope 1](#_Toc68594237)

[4 Roles and Responsibilities 1](#_Toc68594238)

[5 Management Commitment 2](#_Toc68594239)

[6 Authority 3](#_Toc68594240)

[7 Compliance 3](#_Toc68594241)

[8 Policy Requirements 4](#_Toc68594242)

[8.1 System and Services Acquisition Policies and Procedures 4](#_Toc68594243)

[8.2 Allocation of Resources 4](#_Toc68594244)

[8.3 System Development Life Cycle 4](#_Toc68594245)

[8.4 Acquisitions Process 4](#_Toc68594246)

[8.5 Information System Documentation 5](#_Toc68594247)

[8.6 Security Engineering Principles 5](#_Toc68594248)

[8.7 External Information System Services 5](#_Toc68594249)

[8.8 Developer Configuration Management 6](#_Toc68594250)

[8.9 Developer Security Testing and Evaluation 6](#_Toc68594251)

# Introduction

Organization Name has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by Organization Name management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of Organization Name systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies pertain to all Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name systems and our customer's confidential information.

| **Individual or Group** | **Role** | **Responsibility** |
| --- | --- | --- |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for Organization Name information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Manager | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
|  | System Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

Organization Name and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization Name Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these policies is mandatory. It is Organization Name policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Policy Requirements

The following system and services acquisition requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the Organization Name information systems.

## System and Services Acquisition Policies and Procedures

This document is intended to serve as the *System and Services Acquisition Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *System and Services Acquisition Policy* and related controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *System and Services Acquisition Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with Organization Name overall business goals and risk position. Any updates, improvements, or suggestions regarding the *System and Services Acquisition Policy* and/or procedure(s) must be sent to the Information Owner.

## Allocation of Resources

Organization Name must include a determination of information security requirements for information in mission and business process planning. All resources required to protect information bust be identified, documented, and allocated as part of Organization Name capital planning and investment control process. Additionally, a discrete line item must be established for information security in organizational programming and budgeting documentation.

## System Development Life Cycle

Organization Name operates using a Software Development Life Cycle (SDLC) which incorporates information security considerations and integrates the organizational information security risk management process into system development life cycle activities. System security roles, responsibilities, and individuals responsible for information security activities must be defined and documented.

## Acquisitions Process

The following requirements and/or specifications must be included, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

* Security functional requirements and/or specifications
* Security strength requirements
* Security assurance requirements
* Security-related documentation requirements
* Requirements for protecting security-related documentation
* Description of the information system development environment and environment in which the system is intended to operate
* Acceptance criteria

Organization Name developers are required to provide documentation that describes the functional properties of the security controls to be employed in the information system, system component, or information system service being acquired. Design and implementation information of security controls, including security-relevant external system interfaces and high-level design such as configuration changes, change steps, and an architectural summary must also be included in the documentation.

A plan for the continuous monitoring of security control effectiveness that contains at least the minimum FedRAMP requirements in NIST SP 800-53 CA-7 must be developed and documented for the information system, system component, or information system service being acquired. Additionally, early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use must be identified and documented.

Only information technology on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems may be employed.

## Information System Documentation

Organization Name must obtain, protect as required, and make available to authorized personnel, administrator documentation for information that describes:

* Secure configuration, installation, and operation of information
* Effective use and maintenance of security features/functions
* Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions

Organization Name must also obtain, protect as required, and make available to authorized personnel, user documentation for information that describes:

* User-accessible security features/functions and how to effectively use those security features/functions
* Methods for user interaction with information, which enables individuals to use the system in a more secure manner
* User responsibilities in maintaining the security of the information and information system

All attempts to obtain information system documentation when such documentation is either unavailable or nonexistent and creates the document in response must be recorded. The functional properties of the security controls employed within the information system and high-level design information of subsystems and implementation details of security controls must be documented with sufficient detail to permit analysis and testing.

## Security Engineering Principles

Organization Name must apply information system security engineering principles in the specification, design, development, implementation, and modification of information.

## External Information System Services

Organization Name must:

* Require that providers of external information system services comply with organizational information security requirements and employ a moderate control baseline in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance
* Define and document government oversight and user roles and responsibilities with regard to external information system services
* Continuously monitor security control compliance by external service providers
* Conduct an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services
* Ensure that the acquisition or outsourcing of dedicated information security services is approved by appropriate Organization Name personnel
* Require providers of external systems where State information is processed or stored to identify the functions, ports, protocols, and other services required for the use of such services
* Employ organization-defined security safeguards to ensure that the interests of all external systems where State information is processed or stored are consistent with and reflect organizational interests
* Document all existing outsourced security services and conduct a risk assessment of future outsourced security services
* Restrict the location of information processing, information data, and information services to information defined locations

## Developer Configuration Management

Organization Name must require that the developer of the information system, system component, or information system service:

* Perform configuration management during information system design, development, implementation, and operation
* Document, manage, and control the integrity of changes to information configuration items under configuration control
* Implement only organization-approved changes to the system, component, or service
* Document approved changes to the system, component, or service and the potential security impacts of such changes
* Track security flaws and flaw resolution within the system, component, or service and report findings to the Organization Name ISM as well as State customer ISSOs
* Enable integrity verification of software and firmware components

## Developer Security Testing and Evaluation

Organization Name must require developers of the information system, system component, or information system service to partner with security personnel to complete the following activities:

* Create and implement a security test and evaluation plan
* Perform functional, regression, and UAT testing and/or evaluation throughout the Agile development cycle
* Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation
* Implement a verifiable flaw remediation process
* Correct flaws identified during security testing/evaluation
* Perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service

Static code analysis tools will be used to submit a code analysis report as part of the authorization package and in any reporting related to reauthorization requirements. Additionally, Organization Name required developers and information security personnel to document how newly developed code is reviewed in the Continuous Monitoring Plan.