Insert Logo Here

Organization Name

Security Procedures

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 Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68609525)

[2 Purpose 1](#_Toc68609526)

[3 Scope 1](#_Toc68609527)

[4 Roles and Responsibilities 1](#_Toc68609528)

[5 Management Commitment 2](#_Toc68609529)

[6 Authority 3](#_Toc68609530)

[7 Compliance 3](#_Toc68609531)

[8 Procedural Requirements 4](#_Toc68609532)

[8.1 Allocation of Resources 4](#_Toc68609533)

[8.2 Life Cycle Support, Security Engineering Principles 4](#_Toc68609534)

[8.3 Developer Configuration Management and Security Testing 4](#_Toc68609535)

[8.4 Information System Documentation 5](#_Toc68609536)

[8.5 External Information System Services 5](#_Toc68609537)

# Introduction

Organization Name has developed procedures that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These procedures 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

This document defines the information system and services acquisition procedures. These procedures are in place to facilitate the implementation of the Systems and Services Acquisition Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# 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 procedures 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.

# Procedural 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.

## Allocation of Resources

Information security requirements are developed and documented during the planning process for the information system. The {Team/Role}, in coordination with the {Team/Role}are responsible for maintaining the security requirements for the information system on an ongoing basis. These requirements are reviewed annually to ensure the mitigation of current security risks and legal requirements.

Prior to the introduction of a new information system component, the {Team/Role}, in coordination with the {Team/Role}, must ensure the information security requirements are considered and addressed in the planning and certification of the information system.

Organization Name Leadership, in coordination with the {Team/Role}, will, on a yearly basis, ensure that appropriate funding is forecasted and provided for the functions of the {Team/Role}and components utilized by that team, thereby ensuring the protection of the information systems.

The total forecasted funding required ensuring the functions of the {Team/Role}and components utilized by that team, thereby ensuring the protection of the information systems, will include all fully encompassing yearly corporate budget forecasts.

## Life Cycle Support, Security Engineering Principles

The System Development Lifecycle (SDLC) methodology used for the information system is built into the configuration management process through the use of security engineering principles for the development and ongoing maintenance of the information system. The workflows for the SDLC process are managed and tracked within {Tool}.

## Developer Configuration Management and Security Testing

Organization Name has an SDLC process and configuration management policy that includes steps associated and built for security. These processes are performed during development, implementation, and operation of the dotStaff system. All SDLC changes are submitted via {Tool} through {Tool} for approval by the {Team/Role}. All information regarding the change is included in the {Tool} for documentation and tracking purposes.

The SDLC and configuration management documentation includes an in-depth explanation of all approval gates configured within {Tool}. These approval gates ensure integrity of code changes. All code must be peer reviewed and attached to a {Ticket} and approved. To check in and deploy code, someone other than the request must approve to the code to the staging environment.

A release of code through {Tool} to production must be approved by a {Team/Role}. The full Responsible Accountable Consulted Informed (RACI) matrix is located in the development configuration management policy.

All artifacts related to a change are included as a part of the {Ticket} and release in {Tool}. Updates or changes to code are captured by the {Ticket} in {Tool}. Approvals for changes to code are documented in the release in {Tool}.

Organization Name tracks all security flaws and flaw remediation details of the information system within a bug in {Tool}. These are automatically created when the static code scan is run. The static code scan is run twice a week. Scan history is stored within the static code analysis tool.

## Information System Documentation

The {Team/Role} ensures that user documentation, including user-accessible security functions, methods for user interaction and secure access, and user responsibilities is made available. Organization Name {Team/Role}, {Team/Role} and {Team/Role} are responsible for ensuring documentation is available that describes:

* Secure configuration, installation, and operation of the information system
* Effective use and maintenance of security features/functions
* Known vulnerabilities regarding configuration and use of administrative or privileged functions

Access to documentation is controlled through RBAC. Documentation is maintained in {Repository} and access is granted by adding members to the appropriate {Team/Role}.

## External Information System Services

Third-party providers must comply with Organization Name information system security requirements and have deployed security controls that are in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The {Team/Role} ensures the contract contains requirements for adequate security controls and that these controls are documented when contracting with third-party providers.

Organization Name requires that providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services. This information is recorded in Organization Name {Repository}. Organization Name also employs or verifies safeguards on all external information systems where government information is processed or stored.

The external information system services used to support the information system include:

* **{Tool} {Description}**
* **{Tool} {Description}**
* **{Tool} {Description}**
* **{Tool} {Description}**