Insert Logo Here

Organization Name

Security Policy

Maintenance

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 MA Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68593239)

[2 Purpose 1](#_Toc68593240)

[3 Scope 1](#_Toc68593241)

[4 Roles and Responsibilities 1](#_Toc68593242)

[5 Management Commitment 2](#_Toc68593243)

[6 Authority 3](#_Toc68593244)

[7 Compliance 3](#_Toc68593245)

[8 Policy Requirements 4](#_Toc68593246)

[8.1 System Maintenance Policies and Procedures 4](#_Toc68593247)

[8.2 Controlled Maintenance 4](#_Toc68593248)

[8.3 Maintenance Tools 5](#_Toc68593249)

[8.4 Remote Maintenance 5](#_Toc68593250)

[8.5 Maintenance Personnel 5](#_Toc68593251)

[8.6 Timely Maintenance 6](#_Toc68593252)

# 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 security maintenance 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 Maintenance Policies and Procedures

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

The Information Owner will review and update the *System Maintenance 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 Maintenance Policy* and/or procedure(s) must be sent to the Information Owner.

## Controlled Maintenance

Organization Name requires the following actions for all controlled maintenance activities:

* Maintenance and repairs on information components to be scheduled, performed, documented, and records reviewed in accordance with manufacturer or vendor specifications and/or organizational requirements
* All maintenance activities to be approved and monitored, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location
* A designated official to explicitly approve the removal of the information system components from organizational facilities for off-site maintenance or repairs
* Equipment to be sanitized to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs
* All potentially impacted security controls to be checked to verify that the controls are still functioning properly following maintenance or repair actions
* Maintenance records to be maintained and shall include:
  + Date and time of maintenance
  + Name of the individual performing the maintenance and approvers
  + Name of escort, if necessary
  + A description of the maintenance performed and outcome (success/failure)
  + A list of equipment removed or replaced including identification numbers, if applicable

## Maintenance Tools

During all maintenance events, Organization Name must ensure that:

* All information maintenance tools are approved, controlled, and monitored
* All maintenance tools carried into a facility by maintenance personnel are inspected for obvious improper modifications
* All media containing diagnostic and test programs are checked for malicious code before the media are used in the information system
* Unauthorized removal of maintenance equipment is prevented by one of the following:
  + Verifying that there is no organizational information contained on the equipment
  + Sanitizing or destroying the equipment
  + Retaining the equipment within the facility
  + Obtaining an exemption form

## Remote Maintenance

In the event that remote maintenance is required, Organization Name must ensure that:

* Non-local maintenance and diagnostic activities are authorized, monitored, and controlled
* The use of non-local maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system
* Strong identification and authentication techniques are employed in the establishment of non-local maintenance and diagnostic sessions
* Records for non-local maintenance and diagnostic activities are maintained
* All sessions and network connections are terminated when non-local maintenance is completed after connections become inactive
* The establishment and use of non-local maintenance and diagnostic connections are documented in the information System Security Plan

## Maintenance Personnel

In order to further safeguard the information system, Organization Name must ensure that:

* A process for maintenance personnel authorization is established and a current list of authorized maintenance organizations or personnel is maintained
* Personnel performing maintenance on the information system have required access authorizations or are escorted by organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations
* Procedures are implemented for the use of maintenance personnel who lack appropriate security clearances or are not U.S. citizen, that include the following requirements:
  + Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified
  + Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured
* Alternate security safeguards are developed and implemented in the event an information system component cannot be sanitized, removed, or disconnected from the system

## Timely Maintenance

Organization Name must ensure that maintenance support and/or spare parts are obtained for security-critical information system components and/or key information technology components.