

GovRAMP

{Insert Company Name}

Security Policy

Security Maintenance

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

# Table of Contents

[Document Revision History 1](#_Toc196400501)

[Table of Contents 2](#_Toc196400502)

[1 Introduction 3](#_Toc196400503)

[2 Purpose 3](#_Toc196400504)

[3 Scope 3](#_Toc196400505)

[4 Roles and Responsibilities 3](#_Toc196400506)

[5 Management Commitment 4](#_Toc196400507)

[6 Authority 5](#_Toc196400508)

[7 Compliance 5](#_Toc196400509)

[8 Policy Requirements 5](#_Toc196400510)

[8.1 Maintenance Policies and Procedures [MA-1] 5](#_Toc196400511)

[8.2 Controlled Maintenance [MA-2, {MA-2 (2) High Only}] 6](#_Toc196400512)

[8.3 Maintenance Tools [MA-3, MA-3 (1-3)] 6](#_Toc196400513)

[8.4 Non-local Maintenance [MA-4, {MA-4 (3) High Only}] 7](#_Toc196400514)

[8.5 Maintenance Personnel [MA-5, MA-5 (1)] 7](#_Toc196400515)

[8.6 Timely Maintenance [MA-6] 8](#_Toc196400516)

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by {Insert Company Name}’s management and in compliance with the Maintenance family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

# Purpose

The purpose of these policies is to establish Maintenance requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s 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 {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These policies apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

| **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 {Insert Company 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. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | 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 Director | 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 Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company 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 {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company 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
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. 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 {Insert Company Name}’s 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 by an external vendor and/or internal self-assessments 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 Maintenance control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

8.1 Maintenance Policies and Procedures [MA-1]

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

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief privacy officer, ISSO, and/or similar roles or their designees: [MA-1 (a)]

* An organizational-level Maintenance Policy that: [MA-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [MA-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [MA-1 (a) (1) (b)]
* Procedures to facilitate the implementation of Maintenance Policy and the associated Maintenance controls [MA-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the Maintenance policy and procedures. [MA-1 (b)]

{Insert Company Name} must review and update the current Maintenance: [MA-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [MA-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [MA-1 (c) (2)]

8.2 Controlled Maintenance [MA-2, {MA-2 (2) High Only}]

{Insert Company Name} requires the following actions for all controlled maintenance activities:

* Records of maintenance, repairs, and replacements on system components shall be scheduled, documented, and reviewed in accordance with manufacturer or vendor specifications and/or organizational requirements [MA-2 (a)]
* All maintenance activities must be approved and monitored, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location [MA-2 (b)]
* A designated official is to explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance, replacement, or repairs [MA-2 (c)]
* Equipment is to be sanitized to remove all information from associated media prior to removal from organizational facilities for off-site maintenance, replacement, or repairs [MA-2 (d)]
* All potentially impacted security controls are to be checked and verified that the controls are still functioning properly following maintenance, replacement, or repairs [MA-2 (e)]
* Maintenance records are to be maintained and shall include: [MA-2 (f)]
  + Date and time of maintenance
  + Name of the individual performing the maintenance
  + Name of the individual approving the maintenance
  + Name of escort, if necessary
  + Produce an up-to-date and accurate description of the maintenance performed, still in process, and outcome (success/failure)
  + A list of equipment removed or replaced including identification numbers, if applicable

**For high impact systems only:**

* Schedule, conduct, and document maintenance, repair, and replacement actions for the system using configuration management board [MA-2 (2) (a)]
* Automated maintenance must be configured to log when maintenance, repair, or replacement actions occurs using the SIEM tools [MA-2 (2) (b)]

8.3 Maintenance Tools [MA-3, MA-3 (1-3)]

During all maintenance events, {Insert Company Name} must ensure that:

* All information system maintenance tools are approved, controlled, and monitored [MA-3 (a)] followed by review of previously approved system maintenance tools at least annually or upon contract renewal [MA-3 (b)]
* All maintenance tools carried into a facility by maintenance personnel are inspected for improper or unauthorized modifications [MA-3 (1)]
* All media containing diagnostic and test programs are checked for malicious code before the media are used in the information system [MA-3 (2)]
* Unauthorized removal of maintenance equipment is prevented by one of the following:
  + Verifying that there is no organizational information contained on the equipment [MA-3 (3) (a)]
  + Sanitizing or destroying the equipment [MA-3 (3) (b)]
  + Retaining the equipment within the facility [MA-3 (3) (c)]
  + Obtaining an exemption from an Information Security Manager, the Information Owner, or delegated personnel explicitly authorizing removal of the equipment from the facility [MA-3 (3) (d)]

8.4 Non-local Maintenance [MA-4, {MA-4 (3) High Only}]

If remote maintenance is required, {Insert Company Name} must ensure that:

* Non-local maintenance and diagnostic activities are authorized, monitored, and controlled [MA-4 (a)]
* The use of non-local maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system [MA-4 (b)]
* Strong identification and authentication techniques are employed in the establishment of non-local maintenance and diagnostic sessions [MA-4 (c)]
* Records for non-local maintenance and diagnostic activities are maintained [MA-4 (d)]
* All sessions and network connections are terminated when non-local maintenance is completed or after connections become inactive [MA-4 (e)]
* The establishment and use of non-local maintenance and diagnostic connections documented in the System Security Plan

**For high impact systems only:**

* Non-local maintenance and diagnostic services must be performed from a system that implements a security capability comparable to the capability implemented on the system being services [MA-4 (3) (a)]
* Remove the component to be serviced from the system prior to non-local maintenance or diagnostic services; sanitize the component of organizational information before and after the service is performed; and inspect and sanitize the component for any unauthorized software before reconnecting the component to the system [MA-4 (3) (b)]

8.5 Maintenance Personnel [MA-5, MA-5 (1)]

To further safeguard the information system, {Insert Company Name} must ensure that:

* A process for maintenance personnel authorization is established and a current list of authorized maintenance organizations or personnel is maintained [MA-5 (a)]
* Verify that non-escorted personnel performing maintenance have the required access authorizations [MA-5 (b)]
* Designate a technically competent person with the required access authorizations to supervise information system maintenance when the maintenance personnel does not possess the required access authorizations [MA-5 (c)]

**For systems storing or processing Federal or State government information:**

* Procedures are implemented for the use of maintenance personnel who lack appropriate security clearances or are not U.S. citizens, that include the following requirements: [MA-5 (1) (a)]
  + 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 [MA-5 (1) (a) (1)]
  + 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 [MA-5 (1) (a) (2)]
* Alternate security safeguards are developed and implemented in the event an information system component cannot be sanitized, removed, or disconnected from the system [MA-5 (1) (b)]

8.6 Timely Maintenance [MA-6]

{Insert Company Name} must ensure that maintenance support and/or spare parts are obtained for security-critical information system components and/or key information technology components to facilitate recovery within a timeframe to support advertised uptime and availability. [MA-6]