

{Insert CompanY Name}

Security Procedures

System Maintenace [MA]

**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

1 Introduction ............................................................................................................................................. 1

2 Purpose .................................................................................................................................................... 1

3 Scope ........................................................................................................................................................ 2

4 Roles and Responsibilities ........................................................................................................................ 2

5 Management Commitment ..................................................................................................................... 2

6 Authority .................................................................................................................................................. 3

7 Compliance .............................................................................................................................................. 3

8 Procedural Requirements [MA-1] ............................................................................................................ 4

8.1 Control Maintenance [MA-2] ........................................................................................................... 4

8.2 Maintenance Tools [MA-3, MA-3 (1), MA-3 (2), MA-3 (3)] .............................................................. 4

8.3 Non-Local and Remote Maintenance [MA-4] .................................................................................. 5

8.4 Maintenance Personnel [MA-5, MA-5 (1)] ....................................................................................... 5

8.5 Timely Maintenance [MA-6] ............................................................................................................ 5

# 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 Access Control 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 access control 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. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | 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.

# Procedural Requirements [MA-1]

The following identification and authentication requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company Name} information systems.

## Controlled Maintenance [MA-2]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} must schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements. [MA-2 (a)] {Insert Role or Team Name} must approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location. [MA-2 (b)] Require that {Insert Individual or Team Name} explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement. [MA-2 (c)] Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: {Organizational Defined Sanitization Requirements}. [MA-2 (d)] {Insert Individual or Role Name} will check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions. [MA-2 (e)] Include the following information in organizational maintenance records: {Organization-defined Information}. [MA-2 (f)]

## Maintenance Tools [MA-3, MA-3 (1), MA-3 (2), MA-3 (3)]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} must approve, control, and monitor the use of system maintenance tools. [MA-3 (a)] {Insert Individual or Team Name} must review previously approved system maintenance tools at least annually. [MA-3 (b)]

{Insert Individual or Team Name} must inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications. [MA-3 (1)]

{Insert Individual or Team Name} must check media containing diagnostic and test programs for malicious code before the media are used in the system. [MA-3 (2)]

Prevent the removal of maintenance equipment containing organizational information by: [MA-3 (3)]

1. Verifying that there is no organizational information contained on the equipment
2. Sanitizing or destroying the equipment
3. Retaining the equipment within the facility
4. Obtaining an exemption from [FedRAMP Assignment: the information owner] explicitly authorizing removal of the equipment from the facility

## Non-Local and Remote Maintenance [MA-4]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall ensure the following:

1. Approve and monitor nonlocal maintenance and diagnostic activities
2. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system
3. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions
4. Maintain records for nonlocal maintenance and diagnostic activities
5. Terminate session and network connections when nonlocal maintenance is completed

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

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall ensure the following: [MA-5]

1. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel
2. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations
3. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorization

{Insert Company Name} shall ensure the following:

* Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, 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 system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified. [MA-5 (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 system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured
* Develop and implement {Organization-defined Alternate Controls} in the event a system component cannot be sanitized, removed, or disconnected from the system.

## Timely Maintenance [MA-6]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall obtain maintenance support and/or spare parts for {Organization-defined System Components} within {Organization-define timeframe to support advertised uptime and availability} of failure.