Information Technology

System Maintenance

Plan

XX/XX/XXXX

ORGANIZATION NAME

LOGO

Table of Contents

[1. Introduction 3](#_Toc135038747)

[1.2 Compliance with Policies and Regulations 3](#_Toc135038748)

[1.3 Scope for Maintenance 3](#_Toc135038749)

[2. Maintenance Standards 3](#_Toc135038750)

[2.1 PR.MA-1 Maintenance Policy and Procedure (L, M, H) 3](#_Toc135038751)

[2.2 PR.MA-2 Controlled Maintenance (L, M, H) 4](#_Toc135038752)

[2.2.1 PR.MA-2(2) Automated Maintenance (H) 4](#_Toc135038753)

[2.3 PR.MA-3 Maintenance Tools (M, H) 4](#_Toc135038754)

[2.3.1 PR.MA-3(1) Inspect Tools (M, H) 5](#_Toc135038755)

[2.3.2 PR.MA-3(2) Inspect Media (M, H) 5](#_Toc135038756)

[2.3.3 PR.MA-4 Prevent Unauthorized Removal (M, H) 5](#_Toc135038757)

[2.4 PR.MA-4 Nonlocal Maintenance (L, M, H) 5](#_Toc135038758)

[2.4.1 PR.MA-4(3) Comparable Security and Sanitization (H) 5](#_Toc135038759)

[2.5 PR.MA-5 Maintenance Personnel (L, M, H) 5](#_Toc135038760)

[2.5.1 PR.MA-5(1) Individuals Without Appropriate Access (H) 6](#_Toc135038761)

[2.6 PR.MA-6 Timely Maintenance (M, H) 6](#_Toc135038762)

[Risk Acceptance/Policy Exception 6](#_Toc135038763)

[Appendix 7](#_Toc135038764)

[Approval 7](#_Toc135038765)

[Revision History 7](#_Toc135038766)

# Introduction

This IT System Maintenance Plan document provides guidance and standards for securing the ongoing maintenance and upkeep of organizational technology infrastructure. Maintenance activities can introduce risk to an environment and precautions are necessary to maintain the confidentiality, integrity, and availability of systems and data.

## Compliance with Policies and Regulations

This document is designed to ensure that our organization's information technology infrastructure is maintained in a secure, reliable, and efficient manner. As such, this document is developed in compliance with all applicable policies, regulations, and standards.

Our organization is committed to adhering to all relevant laws, regulations, and industry standards related to IT system maintenance, including but not limited to **[Insert requirement or regulation]**, **[Insert requirement or regulation]**, and **[Insert requirement or regulation]**. This document has been developed with these regulations and standards in mind and aims to provide clear and concise guidelines for maintaining our IT systems in accordance with these requirements.

By following the standards outlined in this document, our organization can ensure that we are meeting all applicable requirements for IT system maintenance and that we are maintaining a secure and compliant IT infrastructure. We will regularly review and update this document to ensure that it remains current and aligned with any changes to applicable policies and regulations.

## 1.3 Scope for Maintenance

The IT System Maintenance Standards document is applicable to all IT systems owned by the organization, including servers, desktops, laptops, mobile devices, and network components. For assets not considered property of the organization, other 3rd parties (i.e., agents) may provide maintenance outside the scope of this document.

# Maintenance Standards

The following describes the IT system maintenance controls, which are organized in accordance with NIST guidelines. Each system shall have a categorization level (Low (L), Moderate (M), or High (H)) which relates to the criticality or sensitivity of the asset. L, M, H provides guidance maintenance requirements relative to their asset categorization level aligning to maintain confidentiality, integrity, and availability of systems and data.

## PR.MA-1 Maintenance Policy and Procedure (L, M, H)

The **[Insert department]** will create a clear and accessible maintenance policy for its information systems (e.g., this document). This policy will be distributed to all employees, contractors, and authorized users who have access to systems or information. The policy will cover the purpose, scope, roles, responsibilities, management commitment, coordination among various parts of the organization, and compliance. It will also comply with relevant laws, executive orders, directives, regulations, policies, standards, and guidelines.

The **[Insert title/role of individual acting as CISO]** is responsible for managing the development, documentation, and distribution of this maintenance policy. The policy will be reviewed and updated **[Determine update frequency]**, considering emerging threats, new laws or regulations, changes to existing policies, and advancements in technology. Adjustments will be made based on feedback from key personnel.

System owners and **[Insert title/role of individual reporting to CISO]** in the **[Insert Department Name]** are required to develop, document, and distribute specific procedures for their systems to implement the maintenance policy and associated controls. These procedures will also be reviewed **[Determine update frequency]** and adjusted as needed based on evolving threats, new laws or regulations, changes to policies, and advancements in technology, considering feedback from key personnel.

## PR.MA-2 Controlled Maintenance (L, M, H)

1. Keep a schedule and detailed documentation of maintenance, repairs, and replacements for system components, following the specifications provided by the manufacturer or vendor, and organizational requirements.
2. Provide approval and ongoing monitoring for all maintenance activities, whether they are performed on-site or remotely. This includes overseeing maintenance activities conducted on-site or if the system components are taken to another location for servicing.
3. Ensure that the removal of the system or its components from organizational facilities for off-site maintenance, repair, or replacement is explicitly approved by the system owner, **[Insert title/role of individual reporting to CISO]**, or their designated alternate.
4. Sanitization methods must be used to remove sensitive information from devices prior to being sent off-site for maintenance, repair, or replacement.
5. Verify that all potentially affected controls are still functioning properly after maintenance, repair, or replacement actions.
6. Confirm backups are available if maintenance activities inadvertently cause system and/or data integrity issues.
7. Maintain organizational maintenance records that include the following information:
   1. Date and time of maintenance.
   2. Description of the maintenance performed.
   3. Names of the individuals or group who conducted the maintenance.
   4. Name of the escort involved.
   5. System components or equipment that were removed or replaced.

## PR.MA-2(2) Automated Maintenance (H)

Create and follow established schedules for conducting maintenance, repairs, and replacements for information systems. The use of automated mechanisms must be approved by **[Insert title/role of individual acting as CISO]**. Maintain detailed and up-to-date records for all maintenance, repair, and replacement activities, including requests, scheduled actions, actions in progress, and completed actions. Ensure that the records are accurate, comprehensive, and align with established record retention guidelines.

## PR.MA-3 Maintenance Tools (M, H)

Approval must be granted for the use of system maintenance tools. The actions of the tools shall be monitored to ensure compliance with established policies and procedures. All tools will be assessed **[Determine review frequency]** effectiveness and appropriateness.

## PR.MA-3(1) Inspect Tools (M, H)

All tools providing maintenance capabilities shall be checked for malicious code prior to approval for use. Ongoing inspections such as manual review, malware scans, vulnerability checks, code binary analysis, and/or checksum validations to ensure improper or otherwise unauthorized modifications will be detected.

## PR.MA-3(2) Inspect Media (M, H)

All media containing maintenance tools will be checked for malicious code prior to use.

## PR.MA-4 Prevent Unauthorized Removal (M, H)

The following measures will be taken to prevent unauthorized disclosure of organizational information from maintenance equipment:

1. Inspect the equipment for organizational information prior to its removal.
2. Cleanse or otherwise render contents of the equipment unreadable.
3. Securely store the equipment within the facility to ensure it remains under proper control.
4. Obtain a formal exemption from the **[Insert title/role of individual acting as CISO]**, **[Insert title/role of individual reporting to CISO]** (or their designated alternate), if equipment must be sent and information cannot be properly sanitized.

## PR.MA-4 Nonlocal Maintenance (L, M, H)

The following guidelines are required for nonlocal maintenance (e.g., remote support, diagnostics, updates, etc.):

1. Authorization must be provided prior to granting access.
2. All activities will be monitored through automated or manual methods.
3. It shall be authorized only if it aligns with organizational policies, procedures, and standards.
4. Strong authentication methods must be employed (e.g., MFA, TLS Encryption).
5. Log activity and retain in accordance with retention requirements.
6. Ensure termination of sessions upon completion of activities.

## PR.MA-4(3) Comparable Security and Sanitization (H)

Nonlocal maintenance may be provided by remote systems which may not adhere to the same security standards and could provide access to malicious software.

1. Ensure that the system used to perform nonlocal maintenance and diagnostic services has a security capability comparable to that implemented on the system being serviced.
2. If the security capability cannot be guaranteed on system providing nonlocal maintenance:
   1. Remove the component.
   2. Sanitize the component to remove any organizational information (if applicable).
   3. Thoroughly inspect and sanitize the component upon completion of service.
   4. Re-install the component.

## PR.MA-5 Maintenance Personnel (L, M, H)

The following guidelines ensure that maintenance tasks are authorized, monitored, and conducted securely. This helps to prevent unauthorized access, reduce the risk of system disruptions or compromises, and maintain the overall security and integrity of information systems.

1. Establish processes to authorize maintenance organizations and personnel.
2. Maintain and review lists of all active maintenance organizations and personnel, **[Determine review frequency]**.
3. Grant requisite access.
4. Ensure that personnel assigned to conduct maintenance are authorized in accordance with established procedures.
5. Monitor and supervise maintenance activities.

## PR.MA-5(1) Individuals Without Appropriate Access (H)

Guidelines below address specific requirements for maintenance individuals not formally approved by the organization.

1. Establish processes to address maintenance personnel not formally authorized for access to organizational systems and data.
2. Enforce process methods for non-approved maintenance personnel which maintain confidentiality of organizational information and “least privilege” principles.
3. Active monitoring of activities such as escorting, chaperoning, surveillance, security logging/alerting, and managing maintenance is required.

## PR.MA-6 Timely Maintenance (M, H)

The organization will maintain spare components for the rapid repair of mission critical services and systems or otherwise ensure that supporting maintenance agreements align with internally established availability requirements.

# Risk Acceptance/Policy Exception

Any variations to the guidance provided herein must be formally approved by **[Insert title/role of individual acting as CISO]** for formal acceptance. Supporting documentation may be requested to support a change directive. Formal acceptance will be documented, and any residual risks (if applicable), will be clearly communicated and tracked by the **[Insert title/role of individual acting as CISO]** reporting directly to **[Insert title/role with overall organizational authority]**.

# Appendix

## Approval

This Maintenance Standard document has been reviewed and approved by authorized individuals within the organization. The purpose of this section is to formally indicate that the document has been reviewed and approved by individuals with the necessary expertise and responsibility within the organization.

The following individuals have reviewed and approved this document:

* **[Insert Name, Title, Signature of Approver]**
* **[Insert Name, Title, Signature of Approver]**
* **[Insert Name, Title, Signature of Approver]**

This document was approved on **[Insert Date of Approval]** and will remain in effect until further notice.

The approval section helps establish the authority and validity of the document, provide a record of who reviewed and approved it, and improve accountability within the organization. By approving this document, the organization demonstrates its commitment to ensuring the ongoing maintenance and upkeep of its information technology infrastructure.

## Revision History

The table below provides a summary of changes introduced to this document.

|  |  |  |
| --- | --- | --- |
| Version | Date | Summary of Change |
| 1.0 | **[Insert Date]** | Initial Draft |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |