# System Maintenance Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure Owner |  | Signature: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| Procedure Approver(s) |  |
| Effective Date |  | Next Review Date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage System Maintenance of the IT environment at [COMPANY NAME].

# Scope

This procedure is consistent with CMMC and covers all maintenance procedures within [COMPANY NAME] environment. This procedure will be followed by all employees of [COMPANY NAME]. The CMMC System Security Plan (SSP) will be updated to reflect any significant modifications made to this procedure.

# Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with [COMPANY NAME] through an employee – employer relationship or contract between [COMPANY NAME] and their employer or [COMPANY NAME] and individual.
2. All individuals possessing equipment issued by [COMPANY NAME]
3. All individuals working on the premises of [COMPANY NAME] and/or utilizing the Internet services provided by [COMPANY NAME].

# Governing Laws, Regulations, and Policies

* NIST SP 800-171, 3.7.1 - 3.7.6
* CMMC MA.L2-3.7.1 – MA.L2-3.7.6
* [COMPANY NAME] – MA – 3.7 - System Maintenance Policy

# Procedure Statements

**MA.L2-3.7.1 – Performing maintenance on organizational systems:**

1. Information System maintenance is performed locally by [COMPANY NAME] Systems Group authorized privileged users. Off-site maintenance requires the approval of the <Role> and is limited to printers, copiers, and scanners. All maintenance, repair, or replacement of [COMPANY NAME] system/facility components shall be conducted in accordance with manufacturer or vendor specifications and/or organizational requirements to maintain confidentiality, integrity, and availability. The aforementioned maintenance, repair, or replacements shall be scheduled and documented such that impacts to the organization, information, or employees are those minimally necessary.
   * Documentation and review of records for maintenance repair or replacement on system components performed according to manufacturer or vendor specifications and/or organizational requirements.
   * Monitoring and approval of all maintenance activities, whether performed locally, non-locally (through an external network) or serviced off-site.
   * Review of security controls to verify that the controls are still functioning properly following maintenance or repair actions.
   * Recordation of system/component maintenance as performed to include the following:
     + 1. Date and time of action.
       2. System device identification.
       3. Description of action performed.
2. Type of maintenance includes scheduled and unscheduled maintenance, repair of system components, reconfigurations when required, updates to prevent potential problems, changes to the operating environment, and improvements to operations.
3. Off-site maintenance will only be permitted if required and authorized by the <Role>.

**MA.L2-3.7.2** **- Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance:**

1. All Information System maintenance tools are examined by the <IT Staff>, and the maintenance crew, are inspected for improper or unauthorized modifications, and approved prior to use. Maintenance tools are logically locked using RBAC where the <System Administrator> maintains access or physically locked by the maintenance crew. [COMPANY NAME] does not employ any tools which are outside the organizational boundaries for diagnostic and/or repair actions.
2. Techniques and documentation used to conduct system maintenance are controlled in the company <designated Repository> using RBAC where only authorized individuals who are able conduct system maintenance retain access. The <System Administrator> maintains this list of authorized individuals.
3. Mechanisms (automated scripts, Scheduled jobs, etc) used to conduct system maintenance are controlled in the company <designated Repository> using RBAC where only authorized individuals who are able conduct system maintenance retain access. The <System Administrator> maintains this list of authorized individuals.
4. Personnel used to conduct system maintenance are controlled with Role Based Access Control (RBAC) as implemented with Microsoft Active Directory and with <FSO> approval where only authorized individuals who are able conduct system maintenance retain access. The <System Administrator> maintains this list of authorized individuals. All tools, techniques, and mechanisms are controlled and operated by the [COMPANY NAME] <IT Team>. All system maintenance is controlled and monitored by the <IT Team>. Tools that are used by external personnel working on [COMPANY NAME] systems/facilities are in accordance with applicable standards.

**MA.L2-3.7.3 - Ensure equipment removed for off-site maintenance is sanitized of any CUI:**

1. The maintenance, repair, or replacements shall be scheduled and documented such that impacts to the organization, information, or employees are those minimally necessary. If equipment must be removed for off-site maintenance, the [COMPANY NAME] <Role> ensures that sanitization procedures occur to remove any sensitive information from associated media prior to removal from organizational facilities. Prior to removal, an authorized Privileged User will:

* Sanitize the system or component in accordance with NIST Special Publication 800-88 Revision 1, “Guidelines for Media Sanitization” prior to removal utilizing software that performs a wipe pattern using (insert sanitization tool) that removes the data from the device or by [COMPANY NAME] System Group approved degaussing method.
* Verify that organizational information has been removed from the system or component.
* If any offsite maintenance occurs where sanitization cannot occur, then at minimum, all data contained on the system is encrypted-at-rest and all hard drives will be removed before systems leave the [COMPANY NAME] facility.

**MA.L2-3.7.4** **- Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems:**

1. All media containing diagnostic and testing software are checked by the <Role> for malicious code on an isolated system prior to introducing the tools to the Information System. (malicious code scanning software) scans all software before use on organizational systems. [COMPANY NAME] ensures that all information systems have:
   * The ability to scan diagnostics and test programs for malicious code
   * An updated repository of malicious code signatures

**MA.L2-3.7.5** **- Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete:**

1. All non-local maintenance and diagnostic activities are performed through the enterprise internal network or via external network connections, employing strong authenticators, including multifactor authentication, utilizing Microsoft GCC High and Azure Active Directory.
2. All nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.

* Non-local maintenance (through an external network) and diagnostic activities for Information Systems are only permitted by the <role> and authorized Privileged Users communicating through the Information Systems internal network.
* The use of non-local maintenance and diagnostic tools for the intended repair of Information Systems requires approval from the <role> prior to its use
* All non-local maintenance and diagnostic activities are monitored and are recorded within Microsoft Sentinel.
* All non-local maintenance and diagnostic activities are protected from unauthorized confidentiality and integrity violations using implemented cryptographic mechanisms.

**MA.L2-3.7.6 - Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete:**

1. The <role> or <FSO> will be responsible for the approval of maintenance personnel, such as information technology manufacturers, vendors, consultants, and system integrators. Only company personnel with required access authorizations and technical competence will escort and supervise the maintenance activities of personnel who do not possess the required access authorizations. At the discretion of the <role> and <FSO>, the organization may choose to issue temporary credentials to maintenance personnel based on organizational risk assessments. Temporary credentials will be for a one-time use and only for the duration necessary to complete the maintenance activity.

# Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |

# Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at [COMPANY NAME]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [COMPANY NAME] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 12/5/2022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |