[Insert Company Name and Logo]	
Title: IT System Maintenance	**P&P #:**
Approval Date:	**Review: Annual**
Effective Date:	**Security Team**

Purpose:
This policy establishes the enterprise System Maintenance Policy for managing risks from information asset maintenance and repairs through the establishment of an effective System Maintenance program.

Scope: This policy applies to workstations or servers owned or managed by [Insert Company Name].

Definitions:

1. Information Resources: any items, including telecommunication equipment, computer systems, applications, network equipment, and other equipment, goods, and services related to the processing, storage, transmission and collection of sensitive and regulated data.
2. Information Resource Owners: individual, departments and/or groups with fiscal control over an information resource.
3. Maintenance Activities: any system, configuration, software, and/or hardware changes performed on a [Insert Company name]'s information resource. Such activities encompass both routine maintenance such as updates, patches, and etc., as well as emergency break/fix activities.
4. Maintenance Authorization: formal permission either by an information resource owner or permission stemming from job duties that authorizes an individual to access [Insert Company name]'s information resources and perform maintenance activities.

Policy: [Insert Company name]'s information systems must undergo routine and continued maintenance and upkeep. To determine if changes made to machines were part of the continued system maintenance activities, it is important that such activities be documented. To ensure that routine system maintenance is performed properly, the IT department must ensure that the individuals performing maintenance activities are authorized by [Insert Company name] and have the necessary skills. In addition, the IT department must ensure that the individual tasked with performing maintenance activities either has the authorization to access the information contained on the system or is overseen by an individual with such authorization to help prevent the unauthorized disclosure of sensitive and regulated data.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Procedure:

1. All system maintenance on [Insert Company name] information resource must be coordinated and controlled by the area responsible for the information resources.
2. Maintenance activities must be documented and supervised by [Insert Company name] staff, done in a way that protects information on the information resource from unauthorized disclosures and access, performed by individuals with prior system maintenance authorization, and performed in a timely manner.
3. Responsibilities:
    a. Information Resource Owner
        i. Information Resource Owners are responsible for the development of internal policies and procedures that ensure maintenance activities on the information resources for which they own, and meet the principle responsibilities listed below.
        ii. Information Resource Owners are responsible for ensuring that the individual(s) tasked with performing maintenance activities are authorized to perform such activities and have the necessary knowledge, skills and abilities to adequately perform such activities.
    b. Security Officer
        i. The Security Officer is responsible for reviewing this document no less then annually and making changes, as necessary, to ensure this Policy meets the intended goals of protecting information resources during maintenance activities.
4. Maintenance Control
    a. The IT department has built internal policies, procedures and guidelines to ensure that all information resource maintenance activities are properly scheduled, performed, documented and reviewed to ensure completeness and compliance with any and all applicable local, state and federal laws and contractual obligations.
    b. For all preventative and regular maintenance activities (including repairs) the area responsible for the administration of the information resource must document, at minimum, the following:
        i. The date and time of maintenance
        ii. The name of the individual performing the maintenance
        iii. The company of the individual performing the maintenance if not an [Insert Company name] employee.
            1. The name of the [Insert Company name] employee escorting the individual performing the maintenance, if necessary
            2. Escorts for third-party individuals performing maintenance on [Insert Company name] information resources are required for any maintenance that will take place in restricted access areas

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

        iv. A description of the maintenance performed
        v. A list of all equipment removed and/or replaced, including identification numbers if applicable

    c. For all emergency maintenance activities (including break/fix repair) the area responsible for the administration of the information resource must ensure that maintenance activities are documented following the above guidelines as soon as possible once the emergency maintenance activities are completed.
    d. Internal procedures for information resource maintenance must include requirements for approval for any information resource removal for maintenance/repair activities.
    e. In such circumstances when an information resource must be removed to an off-site repair facility, the area responsible for the information resource must remove any and all sensitive and regulated information using established media sanitization procedures prior to information resource removal.
    f. After maintenance activities, the area responsible for the administration of the information resource must review the operation of the information resource prior to placement back in the production environment to ensure maintenance activities did not negatively impact the security posture of the information resource.

5. Remote Maintenance
    a. The IT department will maintain a list of all individuals with remote access (i.e. any individual with the ability to remotely connect to the information resource from non-[Insert Company name] controlled networks such as the Internet) for maintenance and administration of an information resource.
    b. The IT department allowing remote maintenance of information resources must review the list of individuals granted remote access to determine if such access is still required, at least annually.
    c. Remote maintenance activities must take place through a secured and encrypted protocol (e.g. VPN) when conducted from non-[Insert Company name] controlled networks.
    d. All access accounts for non-[Insert Company name] entities used for maintenance purposes must remain disabled at all times except for those times scheduled and documented as necessary for information resource maintenance, and must be immediately disabled once the scheduled maintenance has been completed.
    e. Any individual engaged in remote maintenance activities must, at the completion of the maintenance task, immediately disconnect from all [Insert Company name] information resources accessed during maintenance activities.
    f. The installation/use of remote maintenance capabilities (e.g. RDP, SSH, etc.) for a [Insert Company name] information resource must be documented by the individual(s) responsible for the ongoing administration of the information

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

resource and kept on file with the rest of the information resource documentation.

6. Maintenance Personnel
    a. Only individuals with permission from the area responsible for administration of an information resource are authorized to perform system maintenance of an information resource.
    b. Individuals granted permission for maintenance of an information resource must, at minimum, be authorized, through a documented job description or other written authorization, by [Insert Company name] to access the information contained on the information resource.
    c. Any individual that does not have [Insert Company name] authorization to access the information contained on an information resource must be supervised by an individual with the appropriate authorization during all phases of system maintenance activities.
7. Timely Maintenance
    a. Whenever possible, areas responsible for critical and/or key information resources should maintain a backup set of hardware and software to enable timely maintenance activities.

Violations:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. The violation may also result in civil and criminal penalties to [Insert Company name] as determined by federal and state laws and regulations related to loss of data.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.