|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Maintenance** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the Cybersecurity Maintenance Policy is to establish a comprehensive framework for maintaining and securing information system components within [Organization Name]. It aims to ensure that all maintenance activities are performed in a controlled manner, safeguarding sensitive data and minimizing risks associated with unauthorized access or data breaches. By outlining procedures for scheduling, documenting, and approving maintenance tasks, the policy seeks to maintain the integrity and functionality of information systems while adhering to manufacturer and organizational standards. Additionally, it addresses the need for secure practices during off-site maintenance, ensuring that sensitive information is sanitized and that proper oversight is in place for all maintenance personnel.

The benefits of the Cybersecurity Maintenance Policy are multifaceted. By enforcing standardized maintenance procedures, the policy enhances the security and reliability of information systems, reducing the likelihood of vulnerabilities that could be exploited during maintenance activities. It fosters accountability through documentation and oversight, ensuring that all maintenance actions are traceable and compliant with organizational standards. Furthermore, by specifying requirements for maintenance tools and personnel, the policy helps to mitigate risks related to malicious code and unauthorized access. Overall, this policy not only protects sensitive information but also promotes operational efficiency and trust in the organization’s cybersecurity posture.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The Maintenance Policy is designed to ensure the secure and efficient maintenance of information system components within [Organization Name]. This policy mandates that all maintenance and repair activities are scheduled, performed, documented, and reviewed according to manufacturer specifications and organizational standards. It emphasizes the need for explicit approval from system owners for off-site maintenance and requires the sanitization of equipment to remove sensitive information prior to its removal from organizational facilities.

The policy outlines stringent controls for maintenance tools, including inspections for unauthorized modifications and checks for malicious code. Additionally, it governs non-local maintenance activities, ensuring that they are conducted securely and monitored appropriately. Authorized personnel are designated to supervise maintenance activities, and timely maintenance support is mandated to uphold operational integrity. Overall, this policy aims to protect information systems from vulnerabilities introduced during maintenance activities while ensuring compliance with security standards and best practices.

* 1. Controlled Maintenance

The [Owner] shall:

1. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or requirements conducted by local IT and/or outsourced IT entities.
2. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
3. Require that system owners explicitly approve the removal of the information system or system components from facilities for off-site maintenance or repairs.
4. Sanitize equipment to remove all information from associated media prior to removal from [Organization Name] facilities for off-site maintenance or repairs.
5. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
6. Include IT and system owner’s defined maintenance-related information in maintenance records.
7. For those components not directly associated with information processing such as scanners, copiers, and printers, maintenance records must include date and time of maintenance, entity performing the maintenance, maintenance performed, components replaced or removed including identification/serial numbers as applicable.
   1. Maintenance Tools

The [Owner] shall:

1. Ensure that system owners and IT approve, control, and monitor information system maintenance tools.
2. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
3. Check media containing diagnostic and test programs for malicious code before the media are used in the information system.
   1. Nonlocal Maintenance

The [Owner] shall:

1. Approve and monitor non-local maintenance and diagnostic activities.
2. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with policy and documented in the security plan for the information system.
3. Employ strong authenticators 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.
6. Document in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.
   1. Maintenance Personnel

The [Owner] shall:

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

The [Owner] shall obtain maintenance support and/or spare parts for information systems as agreed upon within the service level agreement between IT and the system owner.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publications 800-53 – Security and Privacy Controls for Information Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)

[National Institute of Standards and Technology (NIST) Special Publications 800-12 – An Introduction to Information Security](https://csrc.nist.gov/pubs/sp/800/12/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications 800-88 – Guidelines for Media Sanitization](https://csrc.nist.gov/pubs/sp/800/88/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications 800-63 – Digital Identity Guidelines](https://pages.nist.gov/800-63-4/)