|  |  |
| --- | --- |
| **[Organization Name]**  **Information Technology Standard** | **No:** [Policy Number: e.g. POL-GOV-01] |
| **IT Standard**:  **Maintenance Policy** | **Updated:** [Updated Date] |
| **Issued By:** [Authority: e.g. CEO or CIO]  **Owner:** [Owner: e.g. IT Department] |

# 1.0 Purpose and Benefits

# To ensure that Information Technology (IT) resources are maintained in compliance with IT security policies, standards, and procedures.

# 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 [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.

# Information Statement

This policy is applicable to all departments and users of IT resources and assets.

### 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.

### 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.

### 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.

### 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.

### Maintenance Personnel

The [Owner] shall:

1. 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 |
|  |  |

# 8.0 Contact Information

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

[Organization Address & Policy Owner’s Contact Info]

# 9.0 Review and Revisions

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 (SP): NIST SP 800-53 – System Maintenance (MA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-88, NIST SP 800-100; Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 201

[NIST Federal Information Processing Standard (FIPS) Publication 140-2](https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards" \t "_blank)

[NIST Federal Information Processing Standard (FIPS) Publication 198-1](https://csrc.nist.gov/publications/detail/fips/198/1/final)

[NIST Federal Information Processing Standard (FIPS) Publication 180-4](https://csrc.nist.gov/publications/detail/fips/180/4/final)

[NIST Special Publication 800-107, Revision 1, Recommendation for Applications Using Approved Hash Algorithms](https://csrc.nist.gov/publications/detail/sp/800-107/rev-1/final)

|  |  |  |
| --- | --- | --- |
| **Algorithm** | **Minimum Key Length** | **Use Case** |
| AES | 128 | Data Encryption |
| RSA | 2048 | Digital Signatures  Public Key Encryption |
| ECDSA | 256 | Digital Signature  Public Key Encryption |
| SHA | 256 | Hashing |
| HMAC SHA 1 | 112 | Keyed-Hash Message Authentication Code |