5.16 Maintenance (MA) Policy

PURPOSE

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

POLICY

The Maintenance policy addresses the controls that are implemented within systems and organizations. These policies contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policies and procedures. Security and privacy program policies and procedures at the organization level are preferable and may obviate the need for mission- or system-specific policies and procedures.

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

01. Controlled Maintenance

1. The [*IT department*] shall:
2. Schedule, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
3. 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.
4. Require that organizational personnel with information security and privacy responsibilities explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance, repair, or replacement.
5. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance, repair, replacement, or destruction.
6. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance, repair or replacement actions.
7. Include the following information in organizational maintenance records:
	1. Component name.
	2. Component serial number.
	3. Date/time of maintenance.
	4. Maintenance performed.
	5. Name(s) of entity performing maintenance, including escort if required.

02. Maintenance Tools

1. Approve, control, and monitor the use of system maintenance tools.
2. Review previously approved system maintenance tools prior to each use.
3. Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.
4. Check media containing diagnostic and test programs for malicious code before the media are used in the system.
5. Prevent the removal of maintenance equipment containing organizational information by:

* 1. Verifying there is no organizational information contained on the equipment.
	2. Sanitizing or destroying the equipment.
	3. Retaining the equipment within the facility.
	4. Obtaining an exemption from organizational personnel with system maintenance responsibilities explicitly authorizing removal of the equipment form the facility.

03. Nonlocal Maintenance

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.

04. Maintenance Personnel

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 organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

05. Timely Maintenance

1. Obtain maintenance support and/or spare parts for critical system components that process, store, and transmit CJI within agency-defined recovery time and recovery point objectives of failure.

PROCEDURES

Agencies must provide the procedures on how the policies will be implemented.

COMPLIANCE

Agencies are required to review and update the current incident response policy and procedure annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

REFERENCE

CM-8, CP-2, CP-7, RA-7, SA-15, SR-2, SR-3.