Policy #:	Title:	Effective Date:
x.xx	Maintenance Policy	MM/DD/YY

PURPOSE

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

REFERENCE

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

POLICY

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

1. CONTROLLED MAINTENANCE
   IT Department shall:

   a. 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.

   b. 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.

   c. Require that system owners explicitly approve the removal of the information system or system components from facilities for off-site maintenance or repairs.

   d. Sanitize equipment to remove all information from associated media prior to removal from cisecurity facilities for off-site maintenance or repairs.

   e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

   f. Include IT and system owner’s defined maintenance-related information in maintenance records.

g. 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.

2. MAINTENANCE TOOLS
   IT Department shall:

   a. Ensure that system owners and IT approve, control, and monitor information system maintenance tools.

   b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

   c. Check media containing diagnostic and test programs for malicious code before the media are used in the information system.

3. NONLOCAL MAINTENANCE
   IT Department shall:

   a. Approve and monitor non-local maintenance and diagnostic activities.

   b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with policy and documented in the security plan for the information system.

   c. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.

   d. Maintain records for nonlocal maintenance and diagnostic activities.

   e. Terminate session and network connections when nonlocal maintenance is completed.

   f. Document in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

4. MAINTENANCE PERSONNEL
   IT Department shall:

   a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

   b. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations.

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

5. TIMELY MAINTENANCE
   IT Department shall:

   a. Obtain maintenance support and/or spare parts for information systems as agreed upon within the service level agreement between IT and the system owner.

COMPLIANCE

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.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY