1. **Purpose**

<Organization Name> <Insert Organization Mission Here>. 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. The system maintenance program helps <Organization Name> implement security best practices with regard to enterprise system maintenance and repairs.

2. **Scope**

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <Organization Name>. Any information, not specifically identified as the property of other parties, that is transmitted or stored on <Organization Name> IT resources (including e-mail, messages and files) is the property of <Organization Name>. All users (<Organization Name> employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. **Intent**

The <Organization Name> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a system maintenance capability throughout <Organization Name> and its business units to help the organization implement security best practices with regard to enterprise system maintenance and repairs.

4. **Policy**

<Organization Name> has chosen to adopt the System Maintenance principles established in NIST SP 800-53 “System Maintenance,” Control Family guidelines, as the official policy for this domain. The following subsections outline the System Maintenance standards that constitute <Organization Name> policy. Each <Organization Name> Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- **MA-1 System Maintenance Policy and Procedures:** All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

- **MA-2 Controlled Maintenance:** All <Organization Name> Business Systems must:
  - Schedule, perform, document, and review records of maintenance and repairs on information asset components in accordance with manufacturer or vendor specifications and/or organizational requirements.
Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

Requires that a designated official explicitly approve the removal of the information asset or system components from organizational facilities for off-site maintenance or repairs.

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

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

- MA-3 Maintenance Tools: All <Organization Name> Business Systems must approve, control, and monitor the use of information asset maintenance tools.

- MA-4 Non-Local Maintenance: All <Organization Name> Business Systems must:
  - Authorize, monitor, and control non-local maintenance and diagnostic activities.
  - Allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information asset.
  - Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions.
  - Maintain records for non-local maintenance and diagnostic activities.
  - Terminate all sessions and network connections when non-local maintenance is completed.

- MA-5 Maintenance Personnel: All <Organization Name> Business Systems must establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel. In addition, <Organization Name> Business Systems must ensure that personnel performing maintenance on the information asset have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information asset maintenance when maintenance personnel do not possess the required access authorizations.

- MA-6 Timely Maintenance: All <Organization Name> Business Systems must obtain maintenance support and/or spare parts for information systems/assets within defined service level agreements.
Appendix A – References

The following references illustrate public laws which have been issued on the subject of information security and should be used to demonstrate <Organization Name> responsibilities associated with protection of its information assets.


