**IT System Maintenance Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the IT System Maintenance Policy. This policy and procedure establishes the minimum requirements for the IT System Maintenance Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.9 System Maintenance Family, Controls MA-1, MA-2 and MA-5.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The IT System Maintenance Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the system maintenance requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Roles** | Data Owner | System Owner | System Admin | Information Security Officer |
| **Tasks** |   |   |   |   |
| Schedule, perform, document, and review records on maintenance |  |  A | R | R |
| Control all maintenance activities |  | A | R | R |
| Sanitize equipment prior to offsite maintenance |  | A | R | R |
| Checks security controls following maintenance |  | A | R | R |
| Maintain system maintenance records |  | A | R | R |
| Ensure that personnel performing maintenance on the information system have required access authorizations |  | A | R | R |

# STATEMENT OF POLICY

In accordance with SEC501, MA-1, MA-2 and MA-5, “YOUR AGENCY NAME” shall ensure all maintenance, diagnostic, and repair activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability of “YOUR AGENCY NAME”’s information systems.

1. **CONTROLLED MAINTENANCE**
	1. The ISO or designee shall:
		1. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and “YOUR AGENCY NAME” requirements;
		2. Control all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
		3. Explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
		4. Sanitize equipment to remove all information from associated media prior to removal from organizational 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 action; and
		6. Maintain information system maintenance records for the life of the system that include:
			1. Date and time of maintenance.
			2. Name(s) of the individual(s) performing the maintenance.
			3. Name of escort (if necessary).
			4. Description of maintenance performed.
			5. List of equipment removed or replaced (including identification numbers if applicable).
2. **MAINTENANCE PERSONNEL**
	1. The ISO or designee shall ensure that personnel performing maintenance on the information system have required access authorizations or designate organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
		1. Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals.
		2. Third-party maintenance providers under contract to perform maintenance/support services on “YOUR AGENCY NAME” information systems shall provide a list of field service engineers assigned to support “YOUR AGENCY NAME” maintenance contract with the following information for each service representative:
			1. Name,
			2. Company represented,
			3. Title,
			4. Contact Info (phone number; e-mail),
			5. Photo for identification purposes, and
			6. List of systems individual is authorized to perform maintenance on.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO” ““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

 [ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History |
| --- |
| Version | Date | Change Summary  |
| 1 | 07/01/2014 | Original |
| 2 | 11/29/2021 | Formatting changes |