###  IT System Security Planning Policy TEMPLATE

###

**EFFECTIVE DATE: 07/01/2014**

**IT System Security Planning 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” develops, disseminates, and updates the IT System Security Planning Policy. This policy and procedure establishes the minimum requirements for the IT System Security Planning Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.12 Planning Family, controls PL-1, PL-2, PL-3, PL-4, and PL-6 as well as additional Commonwealth of Virginia controls.

# SCOPE

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

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

DoS: Denial of Service

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

LAN: Local Area Network

ROB: Rules of Behavior

SEC501: Information Security Standard 501

SSP: System Security Plan

VCCC: VITA Customer Care Center

“YOUR AGENCY”: “YOUR AGENCY”

# DEFINITIONS

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

# BACKGROUND

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

# 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** | Users | IT Internal Audit Director | System Owner | System Admin | Information Security Officer |
| **Tasks** |   |   |   |   |   |
| Develop a system security plan |  |  |  A |   | I |
| Review and update security plan |  |  | A |  | R |
| Plan, document, and implement additional security controls |  |  | A | R | R |
| Validate and verify compliance |  | A |  |  | I |
| Establish rules of behavior | I |  | I |  | A/R |
| Receive signed acknowledgement from users for rules of behavior | R |  | I |  | A |
| Plan and coordinate security-related activities |  |  | A | R | R |

# STATEMENT OF POLICY

In accordance with SEC501, PL-1, PL-2, PL-3, PL-4 and PL-6 and additional requirements for the Commonwealth of Virginia, “YOUR AGENCY” shall develop and implement a system security plan for each information system classified as sensitive. “YOUR AGENCY” shall establish a set of rules to address a user’s expected behavior with regard to sensitive information and information system usage. “YOUR AGENCY” shall plan and coordinate security-related activities affecting these information systems.

1. **SYSTEM SECURITY PLAN**
	1. The System Owner shall develop a system security plan (SSP) that describes the processes, procedures, and security requirements, and describes the security controls in place or planned for meeting those requirements. The system security plan must adhere to the following requirements:
		1. Is consistent with “YOUR AGENCY”’s enterprise architecture;
		2. Explicitly defines the authorization boundary for the system;
		3. Describes the operational context of the information system in terms of missions and business processes;
		4. Provides the security categorization of the information system including supporting rationale;
		5. Describes the operational environment for the information system;
			1. All IT assets, including hardware, software, and (if appropriate) networking/ telecommunications equipment, must be listed and described.
			2. The description must reflect any environmental or technical factors that are of security significance (e.g., versions, protocols, ports, wireless technology, public access, hosting or operation at a facility outside of the organization’s control), as applicable.
		6. Describes relationships with or connections to other information systems;
			1. The description must include applicable diagrams (e.g., network diagrams, system boundary, interconnections, data flow, and high level design).
		7. Provides an overview of the security requirements for the system;
		8. Is completed based on the results of the risk assessment and describes how existing or planned security controls provide adequate mitigation of risks to which the IT system is subject;
		9. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions and a schedule for implementing planned controls; and
		10. Is reviewed and approved by the Agency Head or ISO prior to plan implementation.
	2. The System Owner shall review the security plan for the information system every year, or more often if necessary due to a material change, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.
	3. The System Owner shall update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
		1. The SSP must be updated when impacted by unforeseen significant events, such as a breach, a new threat, or previously unknown vulnerability.
		2. The SSP must be updated when there is a significant change to the system, including a change in the points of contact, system architecture, system status, system interconnections, or system scope.
		3. The SSP must be updated to factor in planned information system enhancements, to ensure that required security-related activities are planned for in advance.
	4. The System Owner shall plan, document, and implement additional security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.
	5. The “YOUR AGENCY” IT Internal Audit Director is responsible for verifying and validating compliance with the provisions of this policy.
2. **RULES OF BEHAVIOR (ROB)**
	1. The ISO or designee shall:
		1. Establish and make readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
			1. The ROB must include general rules for all users and targeted rules for specific functions such as information system administration, developers, end users, etc.
		2. Receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the ROB before authorizing access to information and the information system;
			1. Electronic signatures are acceptable for use in acknowledging ROB.
		3. Include in the ROB explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information;
		4. Include in the ROB the following information:
			1. Users must store all data files and other critical information on a network share.
			2. Users must store media (diskettes, tapes, and CD-ROM) in a secure location away from extreme temperature and sunlight.
			3. Users must report any apparent or actual resource violation to their supervisor and the VCCC.
		5. Document a “YOUR AGENCY” acceptable use policy, which shall prohibit users from:
			1. Installing or using proprietary encryption hardware/software on “YOUR AGENCY” systems;
			2. Tampering with security controls or tools to inventory hardware or software configured on “YOUR AGENCY” workstations;
			3. Downloading or installing personal software on a “YOUR AGENCY” system, including, but not limited to the following:
				1. Games
				2. Screen Savers
				3. Peer to Peer file-sharing programs
				4. Non-”YOUR AGENCY” supported software
			4. Adding hardware to, removing hardware from, or modifying hardware on a “YOUR AGENCY” system;
			5. Connecting non-”YOUR AGENCY”-owned devices to a “YOUR AGENCY” IT system or network, such as personal computers, laptops, or hand held devices, except in accordance with the current version of the Use of non-Commonwealth Computing Devices to Telework Standard (COV ITRM Standard SEC511);
			6. Storing, using or transmitting copyrighted and licensed materials on “YOUR AGENCY” systems unless the “YOUR AGENCY” owns the materials or “YOUR AGENCY” has otherwise complied with licensing and copyright laws governing the materials;
				1. Users shall acknowledge that the unauthorized duplication and/or violation of the software license agreement for copyrighted software is illegal and subject to disciplinary actions.
			7. Doing certain user activities including, but not limited to:
				1. Using Information System resources for personal gain.
				2. Knowingly introducing:

A virus, or

A computing attack (IP Spoofing or Denial of Service (DoS)).

* + - 1. Using any LAN monitoring device, TCP/IP port scanners, password crackers, keystroke recording programs, protocol analysis software, “hacking tools”, or other port sniffers on the “YOUR AGENCY” LAN;
			2. Setting up or configuring any wireless access points; and
			3. Canceling periodic scans of anti-virus or anti-malware software.
		1. Consult with legal counsel when considering adopting an email disclaimer. Emails sent from “YOUR AGENCY” systems are public records of the Commonwealth of Virginia and must be managed as such.
1. **SECURITY-RELATED ACTIVITY PLANNING**
	1. The System Owner shall plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.
		1. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or non-urgent unplanned) situations.
	2. The System Owner shall identify and coordinate with the stakeholders and participants for each information system and security-related activity; these persons include, but are not limited to, the following:
		1. Business process owners,
		2. Users’
		3. Security personnel,
		4. Operations support personnel, and
		5. Appropriate personnel of connected systems.

Note: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY” 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””)

**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 | Supersedes “YOUR AGENCY” CSRM IT System Security Plan Pol Pro and “YOUR AGENCY” CSRM PC LAN Policy |
| 2 | 11/30/2021 | Formatting changes |