**IT Security Assessment and Authorization 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 standard, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the Security Assessment and Authorization policy. This policy and procedure establishes the minimum requirements for the Security Assessment and Authorization controls.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.4 Security Assessment and Authorization Family, Controls CA-1, CA-3, CA-6, and CA-7, to include specific requirements for the Commonwealth of Virginia in CA-3-COV.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” information and information systems including systems used or operated by contractors and other third parties on behalf of “YOUR AGENCY NAME”

# ACRONYMS

CIO: Chief Information Officer

ISO: Information Security Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

ISA: Interconnection Security Agreement

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 security assessment and authorization program at “YOUR AGENCY NAME” is intended to ensure that necessary security controls are integrated into systems and processes within “YOUR AGENCY NAME”. This policy directs that “YOUR AGENCY NAME” meet the requirements as stipulated by COV ITRM Security Standard SEC501 and security best practices.

# 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** | User  | User Manager | System Owner | System Admin | Information Security Officer |
| **Tasks** |   |   |   |   |   |
| Review and update policy |  |  |   |   | A/R |
| Responsible for documentation and/or isa of dedicated connections between information systems |  |  | A |  R | I |
| Assign an authorizing official for each system |   |   |  |  | A/R |
| Establish a continuous monitoring strategy |   |   |   |   | A/R |

# STATEMENT OF POLICY

In accordance with SEC501, CA-1, CA-3, CA-3-COV, CA-6 and CA-7, Security Assessment and Authorization controls, “YOUR AGENCY NAME” will develop, disseminate, and review/update the Security Assessment and Authorization Policy on an annual basis or more frequently if an operational change is made to a system involved in an interconnection agreement.

1. **INFORMATION SYSTEM CONNECTIONS**

This control applies to dedicated connections between information systems, and does not apply to transitory, user-controlled connections such as email and website browsing.

* 1. Connections from the information system to other information systems outside of the authorization boundary must be authorized by the System Owner through the use of Interconnection Security Agreements (ISAs).
		1. If the connecting systems have the same Authorizing Official, an ISA is not required. Rather, the interface characteristics between the connecting information systems must be described in the security plans for the respective systems.
		2. If the connecting systems have different Authorizing Officials but the Authorizing Officials are in the same organization, “YOUR AGENCY NAME” shall determine whether an ISA is required, or alternatively, the interface characteristics between the connecting information systems must be described in the security plans for the respective systems.

NOTE: Instead of developing an ISA, organizations may choose to incorporate this information into a formal contract, especially if the connection is to be established between an agency and a non-Commonwealth (i.e., private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the connection of the information systems.

* 1. For every sensitive agency IT system that shares data with non-Commonwealth entities, the agency shall require or shall specify that its service provider require:
		1. The System Owner, in consultation with the Data Owner, shall document IT systems with which data is shared. This documentation must include:
			1. The types of shared data;
			2. The direction(s) of data flow; and
			3. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.
		2. The System Owners of interconnected systems must inform one another of connections with other systems.
		3. The System Owners of interconnected systems must notify each other prior to establishing connections to other systems.
		4. The written agreement shall specify if and how the shared data will be stored on each IT system.
		5. The written agreement shall specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data, including but not limited to, Data Breach requirements in the Information Security Standard SEC501.
		6. The written agreement shall specify each Data Owner’s authority to approve access to the shared data.
		7. The System Owners shall approve and enforce the agreement.
	2. Risks that may be introduced when information systems are connected to other systems with different security requirements and security controls must be carefully considered. The Authorizing Official shall determine the risk associated with each connection and the appropriate controls to be employed.
1. **SECURITY AUTHORIZATION**

Security authorization is the official management decision, conveyed through the authorization decision document, given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Commonwealth based on the implementation of an agreed-upon set of security controls.

* 1. For each information system, the ISO or designee shall:
		1. Assign a senior-level executive or manager to the role of authorizing official for the information system;
			1. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems.
			2. Security authorization is an inherently Commonwealth responsibility and therefore, authorizing officials must be Commonwealth employees.
			3. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks.
		2. Ensure that the authorizing official authorizes the information system for processing before commencing operations; and
		3. Update the security authorization at least once a year.
			1. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system.
			2. To reduce the administrative cost of security reauthorization, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision.
1. **CONTINUOUS MONITORING**

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system.

* 1. The ISO or designee shall establish a continuous monitoring strategy and implement a continuous monitoring program that includes:
		1. A configuration management process for the information system and its constituent components;
		2. A determination of the security impact of changes to the information system and environment of operation;
		3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
		4. Reporting the security state of the information system to appropriate organizational officials at least every 120 days.
	2. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package.

# 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 | 11/18/2021 | Formatting changes |