### IT System and Services Acquisition Security Policy TEMPLATE

###

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

**:**

**IT System and Services Acquisition 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 and Services Acquisition Policy. This policy and procedure establishes the minimum requirements for the IT System and Services Acquisition Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.15 IT System and Services Acquisition Family, controls SA-1 through SA-11 as well as additional Commonwealth of Virginia controls.

# 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

SDLC: System Development Life Cycle

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 and Services Acquisition Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the IT system and services acquisition requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all 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** | Data Owner | System Owner | System Admin/Developer | Information Security Officer |
| **Tasks** |   |   |   |   |
| Include requirements in mission/business process planning. |  | A |   | R |
| Determine, document, and allocate resources. |  | A |  | R |
| Manage the information system using sdlc. |  | A |  | R |
| Define and document security roles and responsibilities. |  | A |  | R |
| Identify individual role and responsibilities. |  | A |  | R |
| Follow application planning, development, and support requirements. |  | A | R | R |
| Require system/security documentation. |  | R |  | A |
| Update system/security documentation. |  | A | R | R |
| Ensure that software and documentation are used in accordance with contract agreements. |  | A | R | R |
| Prohibit peer-to-peer file sharing technology. |  |  | E | I/R |
| Require service provider to document its software license management practices. |  |  |  | A/R |
| Enforce explicit rules governing the installation of software by users. |  |  |  | A/R |
| Require that security engineering principles be applied. |  |  | R | A |
| Require that providers of external services comply with “YOUR AGENCY NAME” information security requirements. |  |  |  | A/R |
| Define and document government oversight and user roles and responsibilities for external services. |  |  |  | A/R |
| Monitor and mitigate risks that arise from external services. |  |  |  | A/R |
| Perform configuration management during information system design, development, implementation, and operation. |  | A | R | R |
| Document approved changes. |  | A | R | R |
| Track security flaws and flaw resolution. |  | A | R | R |
| Create and implement a security test and evaluation plan. |  | A | R | R |
| Implement a flaw remediation process. |  | A | R | R |
| Document the results of the security testing and flaw remediation process. |  | A | R | R |
| Perform a vulnerability analysis. |  | A | R | R |

# STATEMENT OF POLICY

In accordance with SEC501, SA-1 through SA-14, “YOUR AGENCY NAME” shall establish the minimum requirements for the IT System and Services Acquisition Policy.

1. **ALLOCATION OF RESOURCES**
	1. The ISO or designee shall:
		1. Include a determination of information security requirements for the information system in mission/business process planning; and
			1. IT security priorities and requirements at the project and enterprise level must be integrated into business cases.
			2. Business case analysis must consider how to employ and leverage existing “YOUR AGENCY NAME” components of the security architecture and standards, including common controls, before new technology control investments may be proposed.
		2. Determine, document, and allocate the resources required to protect the information system as part of its capital planning and investment control process.
2. **LIFE CYCLE SUPPORT**
	1. The ISO or designee shall:
		1. Manage the information system using a system development life cycle (SDLC) methodology that includes information security considerations, as follows:
			1. Project Initiation
				1. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.
				2. Classify the types of data (see IT System and Data Sensitivity Classification) that the IT system will process and the sensitivity of the proposed IT system.
				3. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.
				4. Develop an initial IT System Security Plan (see IT System Security Plans) that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.
			2. Project Definition
				1. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.
				2. Incorporate IT security requirements in IT system design specifications.
				3. Verify that the IT system development process designs, develops, and implements IT security controls that meet information security requirements in the design specifications.
				4. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.
				5. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.
			3. Implementation
				1. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.
				2. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the IT application system.
				3. Require that the system comply with all relevant Risk Management requirements in this Standard.
				4. Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against information security risks, and comply with the other requirements (see IT Systems Security Plans) of this document.
			4. Disposition
				1. Require retention of the data handled by an IT system in accordance with the agency’s records retention policy prior to disposing of the IT system.
				2. Require that electronic media is sanitized prior to disposal, as documented (see Data Storage Media Protection), so that all data is removed from the IT system.
				3. Verify the disposal of hardware and software in accordance with the current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV ITRM Standard SEC514).
			5. Control gates, or established points in the life cycle, must be used to determine whether the project should continue as is, change direction, or be discontinued.
			6. Key outputs, in the form of deliverables or artifacts, for common tasks must be generated.
				1. Expected outputs must provide information vital to the system design.
		2. Define and document information system security roles and responsibilities throughout the system development life cycle;
		3. Identify individuals having information system security roles and responsibilities; and
		4. Implement and document the following requirements:
			1. Application Planning
				1. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.
				2. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete.
				3. Security Requirements – Identify and document the security requirements of the application early in the development life cycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.
				4. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process, or store sensitive information in an application, agencies must address the following design criteria:

Encrypted communication channels shall be established for the transmission of sensitive information;

Sensitive information shall not be visibly transmitted between the client and the application; and

Sensitive information shall not be stored in hidden fields that are part of the application interface.

* + - 1. Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development.

* + - * 1. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.
				2. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.
				3. Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures where possible).
				4. Agencies shall not use or store sensitive data in non-production environments.
				5. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.
				6. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted
				7. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.
				8. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.
				9. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.
			1. Production and Maintenance
				1. Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.
				2. Internet-facing applications classified as sensitive shall have periodic (not to exceed 90 days) vulnerability scans run against the applications and supporting server infrastructure as well as anytime a significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.
1. **INFORMATION SYSTEM DOCUMENTATION**
	1. The ISO or designee shall require:
		1. Administrator documentation (i.e., whether published by a vendor/manufacturer or written in-house) for the information system and constituent components must be obtained, protected as required, and made available to authorized personnel.
			1. Administrator documentation must include information that describes:
				1. Secure configuration, installation, and operation of the information system.
				2. Effective use and maintenance of the system’s security features/functions.
				3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
		2. User documentation (i.e., whether published by a vendor/manufacturer or written in- house) for the information system and constituent components must be obtained, protected as required, and made available to authorized personnel.
			1. User documentation must include information that describes:
				1. User-accessible security features/functions and how to effectively use those security features/functions.
				2. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner.
				3. User responsibilities in maintaining the security of the information and information system.
		3. Security documentation must be updated throughout the information system’s life cycle.
		4. When information system documentation is either unavailable or non- existent, the following actions must be taken:
			1. Document attempts to obtain such documentation.
			2. Recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.
		5. Vendor/manufacturer documentation describing the functional properties of the security controls employed within the information system, with sufficient detail to permit independent analysis and testing, must be obtained, protected as required, and made available to authorized personnel.
		6. Vendor/manufacturer documentation describing the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system, with sufficient detail to permit independent analysis and testing, must be obtained, protected as required, and made available to authorized personnel.
		7. Vendor/manufacturer documentation describing the security-relevant external interfaces to the information system, with sufficient detail to permit independent analysis and testing, must be obtained, protected as required, and made available to authorized personnel.
	2. The ISO or designee shall require that service providers provide assurance that this control is met where applicable.
2. **SOFTWARE USAGE RESTRICTIONS**
	1. The System Owner shall ensure that software and the associated documentation are used in accordance with contract agreements and copyright laws;
		1. Only licensed and registered software may be used on “YOUR AGENCY NAME” information systems.
	2. The ISO or designee shall prohibit the use of peer-to-peer file sharing technology.
	3. “YOUR AGENCY NAME”shall or shall require that its service provider document software license management practices that address the following components, at a minimum:
		1. Require the use of only agency approved software and service provider approved systems management software on IT systems.
		2. Assess periodically whether all software is used in accordance with license agreements.
3. **USER-INSTALLED SOFTWARE**
	1. The ISO or designee shall enforce explicit rules governing the installation of software by users.
		1. Users are prohibited from installing software on “YOUR AGENCY NAME”’s information systems that does not meet one of the following conditions:
			1. The software must conform to Agency-approved standards, including configuration standards.
			2. The installation of non-Agency standard software (including public domain software such as freeware or shareware) must be authorized in writing by the System Owner and the Information Security Officer (ISO).
	2. The System Owner shall ensure the rules of behavior for the information system specify that only authorized software may be installed on “YOUR AGENCY NAME”’s equipment and networks.
	3. “YOUR AGENCY NAME” shall identify the types of software installations that are permitted. Categories of permitted software installations include:
		1. Approved and tested updates and security patches to existing software.
		2. “YOUR AGENCY NAME” developed software.
	4. “YOUR AGENCY NAME” shall identify the types of software downloads that are prohibited. Categories of prohibited software downloads include:
		1. Unauthorized install-on-demand software.
		2. Software whose pedigree with regard to being potentially malicious is unknown or suspect.
		3. Untested unauthorized software.
	5. Rules governing the downloading and installation of software by users must be strictly enforced by information system personnel.
	6. Administrative rights must be removed for any violations of policies and procedures and not restored until appropriate counseling and remediation has taken place.
		1. Administrative rights may be denied in the future.
	7. The information system must be tested for prohibited software by using a scanner which detects and reports the names of installed software and the results must be compared against the approved software applications list.
4. **SECURITY ENGINEERING PRINCIPLES**
	1. The ISO or designee shall require that information system security engineering principles be applied in the specification, design, development, implementation, and modification of the information system.
		1. The application of security engineering principles must be integrated into the SDLC.
		2. Security engineering principles are primarily targeted at information systems under new development and information systems undergoing major upgrades.
		3. For legacy information systems, security engineering principles must be applied to system upgrades and modifications, to the extent feasible, given the current states of the hardware, software, and firmware components within the system.
	2. Security engineering principles must include, but are not limited to:
		1. Developing layered protections.
		2. Establishing sound security policy, architecture, and controls as the foundation for design.
		3. Incorporating security into the SDLC.
		4. Delineating physical and logical security boundaries.
		5. Ensuring system developers and integrators are trained on how to develop secure software.
		6. Tailoring security controls to meet organizational and operational needs.
		7. Reducing risk to acceptable levels, thus enabling informed risk management decisions.
5. **EXTERNAL INFORMATION SYSTEM SERVICES**
	1. The ISO or designee shall:
		1. Require that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable laws, directives, policies, regulations, standards, and guidance;
		2. Define and document government oversight and user roles and responsibilities with regard to external information system services;
			1. Documents that solicit and implement external information system services must:
				1. Identify specific drivers for soliciting the services.
				2. Specify responsibilities for each security control or for specific activities within a control.
				3. Identify associated reporting requirements for each security control.
				4. Require the provider of external information system services to conform to the same security control and documentation requirements as would apply to the “YOUR AGENCY NAME”’s internal systems.
			2. The following documentation must be included in the procurement of external information system services:
				1. Government, service provider, and end user security roles and responsibilities.
				2. Any SLAs.
			3. SLAs must:
				1. Define expectations of performance for each required security control.
				2. Describe measurable outcomes.
				3. Specify remedies and response requirements for any identified instance of non-compliance.
			4. A chain of trust or level of confidence must be established with external service providers to ensure adequate protection of services rendered.
				1. Risks must be assessed in the risk assessment process.
				2. Risks must be documented.
				3. The extent and nature of the chain of trust varies based on the relationship between “YOUR AGENCY NAME” and the external provider.

Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk.

* + 1. Mitigate any risks that arise from the use of external information system services; and
		2. Monitor security control compliance by external service providers.
1. **DEVELOPER CONFIGURATION MANAGEMENT**
	1. The ISO shall require that information system developers/integrators:
		1. Perform configuration management during information system design, development, implementation, and operation for:
			1. Contractual development and system integration.
			2. Internal development procedures.
		2. Manage and control changes to the information system;
		3. Implement only organization-approved changes;
		4. Document approved changes to the information system; and
		5. Track security flaws and flaw resolution.
2. **DEVELOPER SECURITY TESTING**
	1. The ISO or designee shall require that information system developers/integrators, in consultation with associated security personnel (including security engineers):
		1. Create and implement a security test and evaluation plan;
			1. Testing requirements must be included in:
				1. Contractual documents for development and system integration.
				2. Internal development procedures.
			2. The plan must include requirements for retesting after significant changes occur.
		2. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process;
			1. Those controls not in place or not operating as intended, as determined by test results, must be remediated.
		3. Document the results of the security testing/evaluation and flaw remediation processes; and
			1. Developmental security test results, after verification, must be used to the greatest extent feasible;
				1. Use of these test results must include providing evidence for and documenting one of the following:

A control is in place and operating as intended (for a positive test result).

A control is either not in place or not operating as intended (for negative test results).

* + - 1. Developmental security test results must be used in support of the security authorization process for the delivered information system.
				1. Use of these results must be dependent on the following:

How current or recent the test results are.

The judgment of the independent authorization agent as to their applicability.

Note: It must be recognized that these results are impacted (i.e., they many no longer be valid) whenever there have been security-relevant modifications to the information system subsequent to developer testing.

* + 1. Require that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.

# 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 document. |
| 2 | 11/29/2021 | Formatting changes |