**IT Personnel Security 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 Personnel Security Policy. This policy and procedure establishes the minimum requirements for the Personnel Security Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.13 Personnel Security Family, controls PS-1 through PS-8 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 classified as sensitive

# 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 Personnel Security Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary to meet the personnel security 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 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 | Data Owner | System Owner | System Admin | Information Security Officer |
| **Tasks** |  |   |   |   |   |
| Require screening of individuals. |  |  |   |   | A |
| Terminate access and retrieve all organizational property upon termination. |  |  |  | R | A |
| Review and modify logical and physical access authorizations when personnel are reassigned or transferred. |  |  |  | R | A |
| Sign appropriate access agreements. | R |  |  |  | A |
| Review and update access agreements. |  |  |  |  | A/R |
| Establish and document personnel security requirement for third-party providers. |  |  |  |  | A/R |
| Employ a formal sanction process. |  |  |  |  | A/R |

# STATEMENT OF POLICY

In accordance with SEC501, PS-1 through PS-8, “YOUR AGENCY NAME” shall protect sensitive information and information systems by requiring specific procedures for personnel pre-employment, employment, and post-employment.

1. **PERSONNEL SCREENING**
	1. The ISO shall require that:
		1. Individuals must undergo background screening prior to being authorized access to the information system.
		2. Individuals must be rescreened if the length of employment separation exceeds 90 days.
		3. Personnel screening and rescreening must be consistent with applicable state laws, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position.
		4. Components shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.
2. **PERSONNEL TERMINATION**
	1. The ISO shall require upon termination of individual employment:
		1. Information system access is terminated;
			1. If termination is voluntary (i.e., normal, scheduled), terminate information system access within the same day of notification of such termination (i.e., same day the individual is terminated).
			2. If termination is involuntary (i.e., emergency, adverse), terminate information system access within four (4) hours of notification of such termination (i.e., same day the employee is terminated).
		2. All security-related organizational information system-related property is retrieved (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes).; and
		3. Access to organizational information and information systems formerly controlled by terminated individual is retained.
			1. Prior to archiving or permanent disabling of accounts, transfer all “YOUR AGENCY NAME” information to appropriate personnel or archives.
			2. In the event of an adverse removal or involuntary termination, rotate the employee or contractor to a non-sensitive position or restrict access or rights to information systems before notification, whenever possible, to avoid the potential for malicious actions to information systems.
	2. The following activities must be performed for all personnel, including contractors, leaving, changing jobs, or on extended absences:
		1. Change or cancel all passwords, codes, user IDs, and locks.
		2. Disable user IDs for extended absences (60 days).
		3. Update access control lists, mailing lists, etc.
		4. Collect all keys, badges, and similar items.
		5. Reconcile any financial accounts over which the employee had control.
		6. Ensure electronic records are accessible and properly secured, filed, or appropriately disposed.
3. **PERSONNEL TRANSFER**

Note: This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted.

* 1. The ISO shall require that:
		1. Logical and physical access authorizations to information systems and facilities must be reviewed when personnel are reassigned or transferred to other positions within “YOUR AGENCY NAME” and the appropriate actions must be initiated.
			1. The actions undertaken must be driven by the individual’s position risk designation.
		2. The following activities must be performed for all personnel, including contractors, upon personnel reassignment or transfer:
			1. Change or cancel all passwords, codes, and user IDs.
			2. Update access control lists, mailing lists, etc.
			3. Reconcile any financial accounts over which the employee had control.
			4. Ensure electronic records are accessible and properly secured, filed, or appropriately disposed.
			5. Collect old keys, identification cards, authentication tokens, and building passes.
			6. Issue new keys, identification cards, authentication tokens, and building passes.
			7. Close previous information system accounts unless the original supervisor and the new supervisor carefully review the account to ensure that no resources or access privileges are left on the account and the account has only the resources and privileges appropriate to the person’s new role and responsibilities.
			8. Establish new accounts.
				1. The individual’s access privileges and authorizations must be reviewed and updated to be in alignment with the new position on the effective date.
			9. Change information system and facility access authorizations.
				1. Individual information system and facility access authorizations must be reviewed and appropriately aligned or re-aligned with the new position’s required accesses and authorizations.
			10. Provide for access to official records to which the individual employee had access at the previous work location and in the previous information system accounts.
		3. The transfer or reassignment actions must be initiated within 24 hours following the formal transfer action.
		4. Access controls for information systems must be reviewed every 30 days to verify that the access lists have been updated regarding transferred individuals.
1. **ACCESS AGREEMENTS**
	1. The ISO requires that:
		1. Appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) must be signed by individuals requiring access to “YOUR AGENCY NAME” information and information systems prior to being granted access.
			1. Signed access agreements must include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized.
			2. Access agreements must state that penalties for non-compliance may include sanctions and possible criminal and/or civil prosecution.
		2. The access agreements must be reviewed and updated (i.e., redistributed and signatures collected) as follows:
			1. On an annual basis.
			2. Whenever there is a significant change to the information system or information being processed.
			3. Whenever there is a change to the agreements’ verbiage.
		3. An individual’s current, signed access agreements must be kept on file for one fiscal year after termination.

Note: Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by Agency policy.

1. **THIRD-PARTY PERSONNEL SECURITY**
	1. The ISO shall require:
		1. Personnel security requirements including security roles and responsibilities for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management) must be established.
		2. Personnel security requirements must be documented.
			1. Personnel security requirements must be explicitly included in acquisition-related documents.
		3. Provider compliance with personnel security requirements must be monitored.
2. **PERSONNEL SANCTIONS**
	1. The ISO shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.
	2. The sanctions process must be consistent with applicable state laws, directives, policies, regulations, standards, and guidance where applicable.
		1. The sanctions process must also address the following:
			1. Informal corrective actions.
			2. Formal disciplinary actions.
			3. Severe disciplinary actions.
			4. Removal of system access.
			5. Possible criminal and/or civil penalties.
	3. The sanctions process must be described in access agreements.

# 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 | 11/17/2021 | Formatting changes |