3.14 PERSONNEL SECURITY

Quick link to Personnel Security Summary Table

PS-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] personnel security policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Personnel security policy and procedures for the controls in the PS family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

PS-2 POSITION RISK DESIGNATION

Control:

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations [*Assignment: organization-defined frequency*].

Discussion: Position risk designations reflect Office of Personnel Management (OPM) policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the service due to misconduct of an incumbent of a position and establishes the risk level of that position. The PDS assessment also determines if the duties and responsibilities of the position present the potential for position incumbents to bring about a material adverse effect on national security and the degree of that potential effect, which establishes the sensitivity level of a position. The results of the assessment determine what level of investigation is conducted for a position. Risk designations can guide and inform the types of authorizations that individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements. Parts 1400 and 731 of Title 5, Code of Federal Regulations, establish the requirements for organizations to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions.

Related Controls: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.

Control Enhancements: None.

References: [5 CFR 731], [SP 800-181].

PS-3 PERSONNEL SCREENING

Control:

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening*].

Discussion: Personnel screening and rescreening activities reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Related Controls: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

Control Enhancements:

(1) PERSONNEL SCREENING | CLASSIFIED INFORMATION

Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Discussion: Classified information is the most sensitive information that the Federal Government processes, stores, or transmits. It is imperative that individuals have the requisite security clearances and system access authorizations prior to gaining access to such

information. Access authorizations are enforced by system access controls (see AC-3) and flow controls (see AC-4).

Related Controls: AC-3, AC-4.

(2) PERSONNEL SCREENING | FORMAL INDOCTRINATION

Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.

Discussion: Types of classified information that require formal indoctrination include Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartmented Information (SCI).

Related Controls: AC-3, AC-4.

(3) PERSONNEL SCREENING | INFORMATION REQUIRING SPECIAL PROTECTIVE MEASURES

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [*Assignment: organization-defined additional personnel screening criteria*].

Discussion: Organizational information that requires special protection includes controlled unclassified information. Personnel security criteria include position sensitivity background screening requirements.

Related Controls: None.

(4) PERSONNEL SCREENING | CITIZENSHIP REQUIREMENTS

Verify that individuals accessing a system processing, storing, or transmitting [*Assignment: organization-defined information types*] meet [*Assignment: organization-defined citizenship requirements*].

Discussion: None.

Related Controls: None.

References: [EO 13526], [EO 13587], [FIPS 199], [FIPS 201-2], [SP 800-60-1], [SP 800-60-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

PS-4 PERSONNEL TERMINATION

Control: Upon termination of individual employment:

a. Disable system access within [*Assignment: organization-defined time period*];

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

Discussion: System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including

in cases related to the unavailability of supervisors, illnesses, or job abandonment. Exit interviews are important for individuals with security clearances. The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

Related Controls: AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.

Control Enhancements:

(1) PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS

(a) Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and

(b) Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

Discussion: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

Related Controls: None.

(2) PERSONNEL TERMINATION | AUTOMATED ACTIONS

Use [*Assignment: organization-defined automated mechanisms*] to [*Selection (one or more): notify* [*Assignment: organization-defined personnel or roles*] *of individual termination actions*; *disable access to system resources*].

Discussion: In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications, or if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to organizational personnel or roles when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including via telephone, electronic mail, text message, or websites. Automated mechanisms can also be employed to quickly and thoroughly disable access to system resources after an employee is terminated.

Related Controls: None.

References: None.

PS-5 PERSONNEL TRANSFER

Control:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

Discussion: Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within

organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Related Controls: AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.

Control Enhancements: None.

References: None.

PS-6 ACCESS AGREEMENTS

Control:

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements [*Assignment: organization-defined frequency*]; and

c. Verify that individuals requiring access to organizational information and systems:

   1. Sign appropriate access agreements prior to being granted access; and

   2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

Discussion: Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related Controls: AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.

Control Enhancements:

(1) ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION

[Withdrawn: Incorporated into PS-3.]

(2) ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION

Verify that access to classified information requiring special protection is granted only to individuals who:

(a) Have a valid access authorization that is demonstrated by assigned official government duties;

(b) Satisfy associated personnel security criteria; and

(c) Have read, understood, and signed a nondisclosure agreement.

Discussion: Classified information that requires special protection includes collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: None.

(3) ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS

(a) Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and

(b) Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

Discussion: Organizations consult with the Office of the General Counsel regarding matters of post-employment requirements on terminated individuals.

Related Controls: PS-4.

References: None.

PS-7 EXTERNAL PERSONNEL SECURITY

Control:

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [*Assignment: organization-defined time period*]; and

e. Monitor provider compliance with personnel security requirements.

Discussion: External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, information technology services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations. Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

Related Controls: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.

Control Enhancements: None.

References: [SP 800-35], [SP 800-63-3].

PS-8 PERSONNEL SANCTIONS

Control:

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Discussion: Organizational sanctions reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Related Controls: All XX-1 Controls, PL-4, PM-12, PS-6, PT-1.

Control Enhancements: None.

References: None.

PS-9 POSITION DESCRIPTIONS

Control: Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Discussion: Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Related Controls: None.

Control Enhancements: None.

References: [SP 800-181].