**Personnel Security (PS)**

**PS-1: Personnel Security Policy And Procedures**

NIST SP 800-53 Objective: The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]:

a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Control Translation: Ensure personnel security policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the personnel security policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Personnel Security Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**PS-2: Position Categorization**

NIST SP 800-53 Objective: The organization:

a. Assigns a risk designation to all positions;

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

c. Reviews and revises position risk designations

Control Translation: This control is looking to verify that the position risk designations follow OPM guidance and that these requirements guide what type of screening or reviews will be required for each type of position.

Notes: This control may be different for cloud environments run by 3rd parties, however there should still be some sort of differentiation between admin and non-admin roles for example.

How to test and evaluate: Review either a personnel security policy, procedures addressing position categorization, appropriate codes of federal regulations, list of risk designations for organizational positions, security plan, and records of risk designation reviews and updates looking for the differentiation and procedures used within the different roles.

Technology specific: General

**PS-3: Personnel Screening**

NIST SP 800-53 Objective: The organization:

a. Screens individuals prior to authorizing access to the information system; and

b. Rescreens individuals according to an organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening.

Control Translation: This control is looking for the initial screening of users prior to access to the system as well as the conditions and procedures for rescreening.

Notes: The organization may define their own conditions and frequencies for rescreening but this will need to be documented.

How to test and evaluate: Review the personnel security policy, procedures addressing personnel screening, records of screened personnel, and security plan for evidence of the rescreening frequency and rescreening procedures. Review the initial screen procedures and documentation of screens performed for each user to ensure that procedures are being followed.

Technology specific: General

**PS-4: Personnel Termination**

NIST SP 800-53 Objective: The organization, upon termination of individual employment:

a. Terminates information system access;

b. Conducts exit interviews;

c. Retrieves all security-related organizational information system-related property; and

d. Retains access to organizational information and information systems formerly controlled by terminated individual.

Control Translation: This control is looking for the procedures to be used upon employee termination of employment. There should be documentation of what needs to happen in the event of an employee leaving and documentation of the system access removal, exit interview, property retrieval, and who maintains access to the systems and documents created by the departing user.

How to test and evaluate: Review the personnel security policy, procedures addressing personnel termination, records of personnel termination actions, list of information system accounts looking for the procedures to be followed when a user leaves. Make sure to look for documentation of the various items to be completed.

Technology specific: General

**PS-5: Personnel Transfer**

NIST SP 800-53 Objective: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates organization-defined transfer or reassignment actions within an organization-defined time period following the formal transfer action.

Control Translation: This control is similar to PS-4 however this is specific to transitions instead of departures. Make sure to look for documentation of what authorizations are to be reviewed in the event of a transition and what type of job change qualifies as a transition and the timeframe of all actions.

How to test and evaluate: Review the personnel security policy, procedures addressing personnel transfer, security plan, records of personnel transfer actions, and a list of information system and facility access authorizations specifically for evidence of transitions from one position to another in which access authorizations will need to be changed. This may be difficult evidence to find and may result in only reviewing policies to verify.

Technology specific: General

**PS-6: Access Agreements**

NIST SP 800-53 Objective: The organization:

a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and

b. Reviews/updates the access agreements

Control Translation: This control is looking for a signed agreement related to access that is signed by each user. It is also looking for a review/update of each agreement on a regular schedule. This control is related to PL-4 (Rules of Behavior).

Notes: The schedule is usually annually and this is most often covered by a rules of behavior.

How to test and evaluate: Review the personnel security policy, procedures addressing access agreements for organizational information and information systems, security plan, access agreements, records of access agreement reviews and updates reviewing for a signed document that shows an agreement with standards of usage for the system and a process for reviewing and updating this same document with evidence of an acknowledgement of the review by each user.

Technology specific: General

**PS-7: Third-Party Personnel Security**

NIST SP 800-53 Objective: The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Documents personnel security requirements; and

c. Monitors provider compliance.

Control Translation: This control is looking for security requirements specifically for 3rd party providers. It is possible that this control is not applicable if there are no 3rd party providers. Look for procedures to monitor the provider compliance as well if the control is applicable.

Notes: This document could be the same as for internal users, however this document would have to specify that 3rd party providers are covered as well.

How to test and evaluate: Review the personnel security policy, procedures addressing third-party personnel security, list of personnel security requirements, acquisition documents, and compliance monitoring process reviewing for the procedures for 3rd party providers if they are different.

Technology specific: General

**PS-8: Personnel Sanctions**

NIST SP 800-53 Objective: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures

Control Translation: This control is looking for the outcomes or response actions to be taken when a user does not comply with the PS policies we have already reviewed. These could be documented in the rules of behavior documents or via another method. This control is related to PL-4 (Rules of Behavior) and PS-6 (Access Agreements).

How to test and evaluate: Review the personnel security policy, procedures addressing personnel sanctions, rules of behavior, and records of formal sanctions (if applicable) for evidence of actions to be taken and outcomes of those actions.

Technology specific: General