For High-Impact Information Systems

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

PS-1.1 - Examine personnel security policy and procedures, other relevant documents or records, **and**

Interview organizational personnel with personnel security responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents personnel security policy and procedures;				
(ii)	The organization disseminates personnel security policy and procedures to appropriate elements within the organization;				
(iii)	Responsible parties within the organization periodically review personnel security policy and procedures; and				
(iv)	The organization updates personnel security policy and procedures when organizational review indicates updates are required.				

PS-1.2 - Examine personnel security policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with personnel security responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The personnel security policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance;				
(ii)	The personnel security policy is consistent with the organization’s mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(iii)	The personnel security procedures address all areas identified in the personnel security policy and address achieving policy-compliant implementations of all associated security controls.				

PS-2 POSITION CATEGORIZATION - The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [Assignment: organization-defined frequency].

PS-2.1 - Examine personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; OPM policy and guidance; list of risk designations for organizational positions; information system security plan (for organization-defined frequency for review of position categorizations); records of risk designation reviews and updates; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization assigns a risk designation to all positions within the organization;				
(ii)	The organization establishes screening criteria for individuals filling organizational positions;				
(iii)	The risk designations for the organizational positions are consistent with applicable federal regulations and OPM policy and guidance;				
(iv)	The organization defines the frequency of risk designation reviews and updates for organizational positions; and				
(v)	The organization reviews and revises position risk designations in accordance with the organization-defined frequency.				

PS-3 PERSONNEL SCREENING - The organization screens individuals requiring access to organizational information and information systems before authorizing access.

PS-3.1 - Examine personnel security policy; procedures for personnel screening; records of screened personnel; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and				
(ii)	The personnel screening is consistent with appropriate legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.				

PS-4 PERSONNEL TERMINATION - The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

PS-4.1 - Examine personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records, **and**

Interview organizational personnel with personnel security responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization terminates information system access upon termination of individual employment;				
(ii)	The organization conducts exit interviews of terminated personnel;				
(iii)	The organization retrieves all organizational information system-related property from terminated personnel; and				
(iv)	The organization retains access to official documents and records on organizational information systems created by terminated personnel.				

PS-5 PERSONNEL TRANSFER - The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).

PS-5.1 - Examine personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and				
(ii)	The organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.				

PS-6 ACCESS AGREEMENTS -The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [Assignment: organization-defined frequency].

PS-6.1 - Examine personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan (for organization-defined frequency for access agreement reviews); access agreements; records of access agreement reviews and updates; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access;				
(ii)	Organizational personnel sign access agreements;				
(iii)	The organization defines the frequency of reviews and updates for access agreements; and				
(iv)	The organization reviews and updates the access agreements in accordance with the organization-defined frequency.				

PS-7 THIRD-PARTY PERSONNEL SECURITY - The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.

PS-7.1 - Examine personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records, **and**

Interview organizational personnel with personnel security responsibilities; third-party providers to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization establishes 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, networks and security management);				
(ii)	The organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35; and				
(iii)	The organization monitors third-party provider compliance with personnel security requirements.				

PS-8 PERSONNEL SANCTIONS - The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

PS-8.1 - Examine personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and				
(ii)	The personnel sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.				