Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Personnel Security (PS) Procedure

1. PURPOSE

The Environmental Protection Agency (EPA) is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems shall meet the security requirements by implementing the security controls defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

The purpose of this procedure is to facilitate the implementation of the EPA security control requirements for the Personnel Security (PS) control family, as identified in NIST SP 800-53, Revision 5.

2. SCOPE

These procedures address all EPA information and information systems to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. AUTHORITY

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020

5. PROCEDURE

SIO, ISO and EPA SO or their official designees, for EPA-operated systems, and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contractor or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "PS" designator (e.g., PS-2, PS-3) identified for each procedure below corresponds to the NIST- identifier for the Personnel Security control family, as identified in NIST SP 800-53, Revision 5.

NIST defines the applicable PS baseline controls in NIST 800-53B, *Control Baselines for Information Systems and Organizations*. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name. EPA may deviate from the NIST 800-53B Security or Privacy Control Baselines by adding/removing controls or to applicable baselines and are notated with an asterisk.

PS-2 – Position Risk Designation

For All Systems:

1) Assign a risk designation to all organizational positions;
2) Establish screening criteria for individuals filling those positions; and
3) Review and update position risk designations:
   a) As directed by management to meet federal law, mandate, or Agency direction; and
   b) When a new position is defined.

PS-3 – Personnel Screening

For All Systems:

1) Screen individuals prior to authorizing access to the information system; and
2) Rescreen individuals in accordance with conditions requiring rescreening:
   a) Initiate periodic rescreening in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance and the criteria established for the risk designation of the assigned position;
   b) When a change in duty assignment requires a background check as stipulated in policy or law; and
   c) Requests for access to classified information/systems.

PS-4 – Personnel Termination

For All Systems:

1) Upon termination of individual employment:
   a) Disable information system access within:
      i) 4 hours of departure if involuntary termination (i.e., emergency, adverse); and
      ii) The same day of departure if voluntary termination (i.e., normal, scheduled);

b) Terminate or revoke any authenticators and credentials associated with the individual;
c) Conduct exit interviews that include a discussion of continued obligations under information system non-disclosure, confidentiality, and user access agreements, Notify National Security Information (NSI) for users holding a security clearance;
d) Retrieve all security-related organizational information system-related property; and
e) Retain access to organizational information and information systems formerly controlled by terminated individual.

PS-4(2) – Personnel Termination | Automated Actions

For High Systems:

1) Use automated mechanisms to notify Agency-designated officials including appropriate system administrators, SM, ISO, and Information System Security Officers (ISSO), Security Management Division (SMD) and NSI Team (upon termination of an individual holding a security clearance) and disable access to system resources in conjunction with timelines set in PS-4 1)(a) above.

PS-5 – Personnel Transfer

For All Systems:

1) Review and confirm ongoing operational need for current logical and physical access authorizations systems and facilities when individuals are reassigned or transferred to other positions within the organization;
2) Initiate transfer or reassignment actions within 1 business day following formal transfer actions;
3) Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4) Notify Agency-designated officials including appropriate system administrators, SM, ISO and ISSO, SMD and NSI Team (for personnel with a security clearance) upon transfer of an individual within timelines set in PS-4 1) (a) above.

PS-6 – Access Agreements

For All Systems and Privacy Control Baseline:

1) Develop and document access agreements for organizational systems;
2) Review and update the access agreements:
   a) Annually or whenever there is:
      i) A significant change to the information system or information being processed (e.g. new or reduction in data types or categories); and
      ii) A change to the agreements' verbiage; and
3) Verify that individuals requiring access to organizational information and systems:
   a) Sign appropriate access agreements prior to being granted access; and
   b) Re-sign access agreement to maintain access to organizational systems when access agreements have been updated or annually.

PS-7 – External Personnel Security

For All Systems:

1) Establish personnel security requirements, including security roles and responsibilities for external providers;
2) Require external providers to comply with personnel security policies and procedures established by the organization;

3) Document personnel security requirements;
4) Require external providers to notify the SMD, Contracting Officer's Representative (COR), NSI Team (for staff with a security clearance), ISO and the ISSO of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within:
   a) 4 hours for personnel who are being terminated under favorable conditions
   b) 2 hours in the case of personnel who are being terminated under less than favorable conditions (elevated privileges or not); and
5) Monitor provider compliance with personnel security requirements.

PS-8 – Personnel Sanctions

For All Systems:

1) Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and
2) Notify the SMD, NSI Team (for personnel with security clearances), SO, ISO, Information Owners (IO), SMs, Information Resource Management Branch Chiefs (IRMBC), Insider Threat Team in the Office of Homeland Security (OHS), Office of General Council (OGC), the CUI Program Team (for CUI related matters) and Information Management Officers (IMOs) for the system within 4 hours or 2 hours, if the sanctioned individual has a security clearance, when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

PS-9 – Position Descriptions

For All Systems:

1) Incorporate security and privacy roles and responsibilities into organizational position descriptions.

6. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

7. RELATED INFORMATION

- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

8. DEFINITIONS

- **Involuntary Termination** – the employee's departure at the decision of the employer. There are two basic types of involuntary termination, often referred to as being "fired" and "laid off." To be fired, as opposed to being laid off, is generally thought to be the employee's fault and is, therefore, typically considered to be dishonorable and a sign of failure. Being laid off is a result of an organization's strategic, operational or financial decision and such a decision usually affects multiple employees through no fault of their own.

- **Signature (of an individual)** – a mark or sign made by an individual to signify knowledge, approval, acceptance or obligation. Can be accomplished manually, sometimes referred to as a "wet signature," or electronically.
- **External Providers** – external providers include, for example, service bureaus, contractors and other organizations providing information system development, IT services, outsourced applications and network and security management.
- **Voluntary Termination** – a decision made by the employee to leave the job. Such a decision is commonly known as "resignation," "quitting," "leaving" or "giving notice."
- **Written** – or "in writing" means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

9. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes Information Directive: CIO-2150.3-P-13.1 Information Security – Interim Personnel Security Procedures, Version 2.0, July 18, 2012.

11. CONTACTS

For information about this directive, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.12.19 13:55:07 -05'00'

Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management

APPENDIX A: ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
CISO	Chief Information Security Officer
COR	Contracting Officer's Representative
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
IMO	Information Management Officer
IO	Information Owner
IRMBC	Information Resource Management Branch Chiefs
ISO	Information Security Officer
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
NSI	National Security Information
OISP	Office of Information Security and Privacy
OGC	Office of General Counsel
OHS	Office of Homeland Security
OMB	Office of Management and Budget
OMS	Office of Mission Support
PS	Personnel Security
SIO	Senior Information Official
SM	Service Manager
SMD	Security Management Division
SO	System Owner
SP	Special Publication
U.S.C.	United States Code