Information Technology (IT) Personnel Security (PS) Standard

January 31, 2023

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **IAS_Governance@ed.gov.**

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.01.30 15:22:26 -05'00'

Steven Hernandez

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Table 1: Revision History

Version	Date	Summary of Changes
1.0	1/18/2022	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.
1.2	1/31/2023	Annual review; update broken links and add footnote to HVA control reference in Section 2. Remove PS-1 from privacy baseline.

Contents

1 INTRODUCTION

This governance document establishes Department information technology (IT) system maintenance controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing regulation Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as baseline information system controls.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these personnel security standards.

2 STANDARDS

The Department standards for IT personnel security controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

for Department information systems, a FIPS 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline. In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay[5] issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

This standard directly supports the Department's integration of the NIST Cyber Security Framework (CSF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to Appendix A for a summary of controls by baseline and corresponding NIST CSF categories and subcategories.

2.1 PS-1 Policy and Procedures (L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy* a Department-level IT Personnel Security policy (e.g., OM: 4-114/ACSD-OFO-031, *Physical Security Program*; OFO-O: 5-102/ACSD-OFO-017, *Federal Employee Personnel Security Screening*; OFO-O: 5-101/ACSD-OFO-013, *Contractor Employee Personnel Security Screenings;* OM: 3-104/ ACSD-OFO-011 *Clearance of Personnel for Separation or Transfer*; and this document) that:

a. address's 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.

c. authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy*.

The Department CISO in conjunction with Physical Security Officer are designated to manage the development, documentation, and dissemination of the Department-level IT personnel security

[5] https://www.cisa.gov/publication/high-value-asset-control-overlay

policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office (PO) Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of the Department's IT Personnel Security policy and the associated controls. The ISO and ISSO shall review IT Personnel Security procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 PS-2 Position Risk Designation (L, M, H)

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:

    1. Every five (5) years for federal employees; and

    2. During contract solicitation for contractors in accordance with OFO-O: 5-101/ACSD-OFO-013, *Contractor Employee Personnel Security Screenings*.

2.3 PS-3 Personnel Screening (L, M, H)

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

b. Rescreen individuals in accordance with requirements specified in OFO-O: 5-102 *Federal Employee Personnel Security Screening* and OFO-O: 5-101 *Contractor Employee Personnel Security Screenings.*

2.4 PS-4 Personnel Termination (L, M, H)

Upon termination of individual employment:

a. Disable system access as soon as possible but no later than one business day after notifying the Help Desk

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

c. Conduct exit interviews that include a discussion of topics to include but not limited to:

    1. Security constraints
    2. Proper accountability
    3. Nondisclosure agreements; and
    4. Limitations on future employment.

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

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

2.4.1 PS-4(2) Personnel Termination | Automated Actions (H)

Use ED approved automated mechanisms to:

a. Notify personnel with separation responsibilities as defined in the ED OM: 3-104/ ACSD-OFO-011 *Clearance of Personnel for Separation or Transfer* of individual termination actions; and

b. Disable access to system resources.

2.5 PS-5 Personnel Transfer (L, M, H)

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 ED transfer or reassignment actions within five (5) business days 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 ED personnel and/or roles as defined in the OM: 3-104/ ACSD-OFO-011 *Clearance of Personnel for Separation or Transfer* within twenty-four (24) hours.

2.6 PS-6 Access Agreements (P, L, M, H)

a. Develop and document access agreements for organizational systems

b. Review and update the access agreements at least annually (i.e., each fiscal year); 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 at least annually (i.e., each fiscal year).

2.7 PS-7 External Personnel Security (L, M, H)

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 the Contracting Officer Representative (COR), key personnel, and personnel with privileged access, of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within twenty-four (24) hours to forty-eight (48) hours; and

e. Monitor provider compliance with personnel security requirements.

2.8 PS-8 Personnel Sanctions (L, M, H)

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

b. Notify all appropriate personnel and offices, to include but not limited to Personnel Security, OFO/OHR, OCIO, COR and/or supervisors or employee representatives, as appropriate within twenty-four (24) hours to forty-eight (48) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

2.9 PS-9 Position Descriptions (L, M, H)

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

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

APPENDIX A: ACRONYMS

Table 2: Acronym List

Acronym	Description
ACS	Administrative Communications Service
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COR	Contracting Officer's Representative
ED	Department of Education
EO	Executive Order
FIPS	Federal Information Processing Standard
HVA	High Value Asset
IAS	Information Assurance Services
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OFO	Office of Finance and Operations
OMB	Office of Management and Budget
PO	Principal Office
PS	Personnel Security
SAOP	Senior Agency Official for Privacy
SP	Special Publication

APPENDIX B: BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray and notated with an asterisk.

Table 3: Baseline Control Parameter Summary

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
PS-1	Policy and Procedures		x	x	x	PR.IP, DE.DP, GV.PO-P, GV.MT-P, PR.PO-P	PR.IP-11, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P9
PS-2	Position Risk Designation		x	x	x	PR.IP, PR.PO-P	PR.IP-11, PR.PO-P9
PS-3	Personnel Screening		x	x	x	PR.AC, PR.IP, PR.PO-P, PR.AC-P	PR.AC-6, PR.IP-11, PR.PO-P9, PR.AC-P6
PS-4	Personnel Termination		x	x	x	PR.IP, PR.PO-P	PR.IP-11, PR.PO-P9
PS-4(2)	Personnel Termination | Automated Actions				x	PR.IP, PR.PO-P	PR.IP-11, PR.PO-P9
PS-5	Personnel Transfer		x	x	x	PR.IP, PR.PO-P	PR.IP-11, PR.PO-P9
PS-6	Access Agreements	x	x	x	x	PR.DS, PR.IP, PR.PO-P, PR.DS-P	PR.DS-5, PR.IP-11, PR.PO-P9, PR.DS-P5
PS-7	External Personnel Security		x	x	x	ID.AM, ID.GV, ID.SC, PR.AT, PR.IP, DE.CM, ID.DE-P, GV.PO-P, GV.AT-P, PR.PO-P	ID.AM-6, ID.GV-2, ID.SC-4, PR.AT-3, PR.IP-11, DE.CM-6, ID.DE-P5, GV.PO-P3, GV.AT-P4, PR.PO-P9
PS-8	Personnel Sanctions		x	x	x	PR.IP, PR.PO-P	PR.IP-11, PR.PO-P9
PS-9	Position Descriptions		x	x	x	ID.GV, PR.IP, GV.PO-P, PR.PO-P	ID.GV-2, PR.IP-11, GV.PO-P3, PR.PO-P9