Information Technology (IT) Personally Identifiable Information Processing and Transparency (PT) Standard

January 26, 2024

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: 2024.01.26 17:03:42 -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.

Version	Date	Summary of Changes
1.0	1/18/2022	Initial draft of new standard which combines Technology (NIST) Special Publication (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	1/30/2023	Annual review; no updates required.
5.3	1/30/2024	Aligned document major version number to align with National Institute of Standards and NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Updated Version 1.2 revision date to align with signature date of 1/30/2023 in the revision history. Inserted references to NIST SP 800-53B tailoring guidance. Updated Section 4, Acronyms as appropriate. Updated language in controls PT-01 and PT-06. Added controls PT-03(01), PT-03(02), PT-04(01), PT-04(02), PT-04(03), and PT-05(01). Rescinded control PT-06 ED-01. Added “leading zeros” to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays. Updated baseline Control Parameter Summary Table to scope into the Privacy baseline control enhancements PT-04(01), PT-04(02), PT-04(03), and PT-05(01) in accordance with guidance from the Privacy Office.

Table of Contents

1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) personally identifiable information processing and transparency controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders (EO), Emergency Orders, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. 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 governance 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 (PUB) 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 amended, 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 personally identifiable information processing and transparency control standards.

[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/sites/whitehouse.gov/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

2 STANDARDS

The Department standards for IT system personally identifiable information processing and transparency 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 for Department information systems, a FIPS PUB 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 PUB 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 U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[6], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[7].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

This standard directly supports the Department's integration of the NIST Cybesecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to *APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY* for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

[5] CISA HVA Overlay https://www.cisa.gov/publication/high-value-asset-control-overlay
[6] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf
[7] FedRAMP baselines https://www.fedramp.gov/baselines/

2.1 PT-01 Policy and Procedures (P)

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 ACSD-OCIO-004[8], *Cybersecurity Policy* a Department-level personally identifiable information processing and transparency policy (e.g., this document) 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.

(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 ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Department Senior Agency Official for Privacy (SAOP) is designated to manage the development, documentation, and dissemination of the Department-level personally identifiable information processing and transparency 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.

The Department-level personally identifiable information processing and transparency standard operating procedures 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.

[8] Also known as OCIO: 3-112

2.2 PT-02 Authority to Process Personally Identifiable Information (P)

a. Determine and document the authority as defined in the Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), and/or System of Records Notice (SORN) for the system that permits the processing of personally identifiable information; and

b. Restrict the processing as defined in the PTA, PIA, and/or SORN of personally identifiable information to only that which is authorized.

2.3 PT-03 Personally Identifiable Information Processing Purposes (P)

a. Identify and document the purposes for processing personally identifiable information;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the processing of personally identifiable information to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing personally identifiable information and implement mechanisms as defined in the PTA, PIA, and/or SORN to ensure that any changes are made in accordance with existing ED privacy policies.

2.3.1 PT-03(01) Personally Identifiable Information Processing Purposes | Data Tagging

Attach data tags containing the following purposes to to personally identifiable information elements defined in the PTA, PIA, and/or SORN: regulating, controlling, and processing personally identifiable information identified in the PTA, PIA, and/or SORN by the information system.

2.3.2 PT-03(02) Personally Identifiable Information Processing Purposes | Automation

Track processing purposes of personally identifiable information using an automated tool.

2.4 PT-04 Consent (P)

Implement mechanisms as defined in the PTA, PIA, and/or SORN for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

2.4.1 PT-04(01) Consent | Tailored Consent (P)

Provide mechanisms as defined in the PTA, PIA, and/or SORN to allow individuals to tailor processing permissions to selected elements of personally identifiable information.

2.4.2 PT-04(02) Consent | Just-in-Time Consent (P)

Present mechanisms as defined in the PTA, PIA, and/or SORN to individuals at the point of collection and in conjunction with personally identifiable information processing as defined in the PTA, PIA, and/or SORN.

2.4.3 PT-04(03) Consent | Revocation (P)

Implement mechanisms as defined in the PTA, PIA, and/or SORN for individuals to revoke consent to the processing of their personally identifiable information.

2.5 PT-05 Privacy Notice (P)

Provide notice to individuals about the processing of personally identifiable information that:

a. Is available to individuals upon first interacting with an organization, and subsequently at the point when changes to the processing of PII requires notification;

b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;

c. Identifies the authority that authorizes the processing of personally identifiable information;

d. Identifies the purposes for which personally identifiable information is to be processed; and

e. Includes other information as stated in the PTA, PIA, and/or SORN.

2.5.1 PT-05(01) Privacy Notice | Just-In-Time Notice (P)

Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or immediately prior to the point of collection.

2.5.2 PT-05(02) Privacy Notice | Privacy Act Statements (P)

Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

2.6 PT-06 System of Records Notice (P)

For systems that process information that will be maintained in a Privacy Act system of records:

a. Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;

b. Publish system of records notices in the Federal Register; and

c. Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

Control Overlay PT-06 ED-01: Reserved; withdrawn due to redundancy with Control PT-06.

2.6.1 PT-06(01) System of Records Notice | Routine Uses (P)

Review all routine uses published in the system of records notice at least biennially to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

2.6.2 PT-06(02) System of Records Notice | Exemption Rules (P)

Review all Privacy Act exemptions claimed for the system of records at least biennially to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

2.7 PT-07 Specific Categories of Personally Identifiable Information (P)

Apply any processing conditions as defined in the PTA, PIA, and/or SORN for specific categories of personally identifiable information.

2.7.1 PT-07(01) Specific Categories of Personally Identifiable Information | Social Security Numbers (P)

When a system processes Social Security numbers:

a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

b. Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and

c. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

2.7.2 PT-07(02) Specific Categories of Personally Identifiable Information | First Amendment Information (P)

Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

2.8 PT-08 Computer Matching Requirements (P)

When a system or organization processes information for the purpose of conducting a matching program:

a. Obtain approval from the Data Integrity Board to conduct the matching program;

b. Develop and enter into a computer matching agreement;

c. Publish a matching notice in the Federal Register;

d. Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and

e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

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).

4 ACRONYMS

Acronym	Definition
ACSD	Administrative Communications System Directive
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CM.AW-P	Data Processing Awareness
CM.PO-P	Communication Policies, Processes, and Procedures
CM-P	Communicate-P
CSF	Cybersecurity Framework
CT.DM-P	Data Processing Management
CT.PO-P	Data Processing Policies, Processes, and Procedures
CT-P	Control-P
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
ED	U.S. Department of Education
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Process Standard
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
GV.MT-P	Monitoring and Review
GV.PO-P	Governance Policies, Processes, and Procedures
GV-P	Govern-P
H	High
HVA	High Value Asset
IAS	Information Assurance Services
ID.IM-P	Inventory and Mapping
ID.RA-P	Risk Assessment
ID-P	Identify-P
IRS	Internal Revenue Service
IT	Information Technology
L	Low
M	Moderate
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameter
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PT	Personally Identifiable Information Processing and Transparency Family
PUB	Publication

Acronym	Definition
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy
SP	Special Publication
SSN	Social Security Number

APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

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
PT-01	Policy and Procedures	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CM.PO-P, GV.PO-P, GV.MT-P	ID.IM-P5, CT.PO-P1, CT.PO-P3, CM.PO-P1, CM.PO-P2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6
PT-02	Authority to Process Personally Identifiable Information	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-02(01)	Authority to Process Personally Identifiable Information | Data Tagging		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-02(02)	Authority to Process Personally Identifiable Information | Automation		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-03	Personally Identifiable Information Processing Purposes	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-03(01)	Personally Identifiable Information Processing Purposes | Data Tagging		Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1
PT-03(02)	Personally Identifiable Information Processing Purposes | Automation		Not allocated to security	Not allocated to security	Not allocated to security	ID.IM-P, CT.PO-P, CT.DM-P, CM.PO-P	ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1

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
			control baselines	control baselines	control baselines		
PT-04	Consent	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CT.PO-P, CM.AW-P	CT.PO-P1, CT.PO-P3, CM.AW-P8
PT-04(01)	Consent | Tailored Consent	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CT.PO-P, CM.AW-P	CT.PO-P1, CT.PO-P3, CM.AW-P8
PT-04(02)	Consent | Just-in-time Consent	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CT.PO-P, CM.AW-P	CT.PO-P1, CT.PO-P3, CM.AW-P8
PT-04(03)	Consent | Revocation	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CT.PO-P, CM.AW-P	CT.PO-P1, CT.PO-P3, CM.AW-P8
PT-05	Privacy Notice	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P, CM.AW-P	CM.PO-P1, CM.AW-P1, CM.AW-P3
PT-05(01)	Privacy Notice | Just-in-time Notice	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P, CM.AW-P	CM.PO-P1, CM.AW-P1, CM.AW-P3
PT-05(02)	Privacy Notice | Privacy Act Statements	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P, CM.AW-P	CM.PO-P1, CM.AW-P1, CM.AW-P3
PT-06	System of Records Notice	X	Not allocated to security	Not allocated to security	Not allocated to security	CM.PO-P	CM.PO-P1

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
			control baselines	control baselines	control baselines		
PT-06(01)	System of Records Notice | Routine Uses	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P	CM.PO-P1
PT-06(02)	System of Records Notice | Exemption Rules	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	CM.PO-P	CM.PO-P1
PT-07	Specific Categories of Personally Identifiable Information	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, ID.RA-P	ID.IM-P6, ID.RA-P1
PT-07(01)	Specific Categories of Personally Identifiable Information | Social Security Numbers	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, ID.RA-P	ID.IM-P6, ID.RA-P1
PT-07(02)	Specific Categories of Personally Identifiable Information | First Amendment Information	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines	ID.IM-P, ID.RA-P	ID.IM-P6, ID.RA-P1
PT-08	Computer Matching Requirements	X	Not allocated to security control baselines	Not allocated to security control baselines	Not allocated to security control baselines		