# Information Technology (IT) Planning (PL) Standard

**November 17, 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 **OCIO_IAS@ed.gov**

# APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.11.17 17:12:05 -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 | 12/22/2021 | 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 | 1/14/2022 | Update to incorporate feedback from Information Assurance Services (IAS), Governance, Risk and Policy (GRP) Team. |
| 1.2 | 1/31/2022 | Update to incorporate feedback from IAS and address new security measures required by Executive Order (EO) 14028, and OMB regulations and memoranda and updated NIST guidance issued in response to EO 14028. |
| 1.3 | 2/11/2022 | Appendix B updated to clarify exceptions to required authorization documentation. |
| 1.4 | 3/29/2022 | Control Overlay PL-2 ED-03 and Appendix B updated to clarify exceptions to required authorization documentation. |
| 1.5 | 4/8/2022 | Added Control Overlay PL-8(1) ED-01 for High Value Assets (HVA) systems. Updated to include feedback from GRP Security Assessment Team (SAT). |
| 1.6 | 06/30/2022 | Update to remove the Cybersecurity & Infrastructure Security Agency (CISA) HVA Overlay. |
| 1.7 | 12/02/2022 | Updated Appendix B requirements for Disaster Recovery Plan (DRP) and Disaster Recovery Plan Test (DRPT). |
| 5.8 | 11/17/2023 | Aligned document major version number to align with 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 Section 4, Acronyms as appropriate. Updated language in controls PL-1, PL-02 ED-05, PL-02 ED-06, PL-02 ED-08, PL-04 ED-01, PL-4(1), and PL-4(1) ED-01. Added control PL-8(1). Added “leading zeros” to control identifiers in alignment with patch |

| Version | Date | Summary of Changes |
|---|---|---|
| | | release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays. |

# Table of Contents

# 1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) planning 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 Directives, 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 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 (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 planning 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/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

# 2 STANDARDS

The Department standards for IT system planning 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 PUB 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 Overlays[5] issued and maintained by the U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax return information (FTRI) 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 Cybersecurity 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.

## 2.1 PL-01 Policy and Procedures (P, 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

[5] HVA Control 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/

of ED, or ED information as defined in ACSD-OCIO-004[8], *Cybersecurity Policy* a Department-level IT system planning policy (e.g., this document) that:

(a) addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

(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 Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT system planning 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 Information System Owners (ISOs) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of this policy standard and associated IT system planning controls. The ISO and ISSO shall review 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 PL-02 System Security and Privacy Plans (P, L, M, H and Control Overlay)

a. Develop security and privacy plans for the system that:

    1. Are consistent with the organization's enterprise architecture.

    2. Explicitly define the constituent system components.

[8] Also known as OCIO: 3-112.

3. Describe the operational context of the system in terms of mission and business processes.
4. Identify the individuals that fulfill system roles and responsibilities.
5. Identify the information types processed, stored, and transmitted by the system.
6. Provide the security categorization of the system, including supporting rationale.
7. Describe any specific threats to the system that are of concern to the organization.
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information.
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components.
10. Provide an overview of the security and privacy requirements for the system.
11. Identify any relevant control baselines or overlays, if applicable.
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions.
13. Include risk determinations for security and privacy architecture and design decisions.
14. Include security- and privacy-related activities affecting the system that require planning and coordination with other individuals or groups within the organization, including but limiting to, those responsible for assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing, as required.
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to personnel with cybersecurity and privacy responsibilities, including but not limited to the Authorizing Official (AO) or AO delegate, ISSO, and ISO.

c. Review the plans at least annually or when a major change occurs to the system.

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments.

e. Protect the plans from unauthorized disclosure and modification.

***Control Overlay PL-02 ED-01 (L, M, H):*** Designate the Cyber Security Assessment and Management (CSAM) tool as the authoritative source for developing, managing and maintaining the Department's IT systems; the system of record for FISMA reporting; and the enterprise tool used to support Assessment and Authorization processes.

***Control Overlay PL-02 ED-02 (L, M, H):*** Use CSAM to generate the system security plan (SSP); not required for cloud service providers or Shared Services.

***Control Overlay PL-02 ED-03 (L, M, H):*** Use the current version of the SSP Review Checklist to document the SSP meets the minimum requirements for signature; not required for cloud service providers, Shared Services, or Office of the Inspector General (OIG).

***Control Overlay PL-02 ED-04 (L, M, H):*** Digitally sign the CSAM generated SSP signature page to document SSP approval. Require signatures from the ISO and ISSO with the AO or AO delegate signature required only if it is the first time the SSP is generated (initiation) or if there is a major change. Not applicable for cloud service providers or Shared Services.

***Control Overlay PL-02 ED-05 (L, M, H):*** Complete all required authorization documentation shown in *APPENDIX B: REQUIRED NARRATIVES, APPENDICES, AND OTHER DOCUMENTATION* as well as all fields within CSAM, including control implementation statements, prior to the issuance of an initial Authorization to Operate (ATO).

***Control Overlay PL-02 ED-06 (L, M, H):*** Review, update and maintain throughout the system lifecycle accurately completed required authorization documentation in accordance with *APPENDIX B: REQUIRED NARRATIVES, APPENDICES, AND OTHER DOCUMENTATION* to support continuous monitoring and ongoing authorization.

***Control Overlay PL-02 ED-07 (L, M, H):*** Review, update and maintain the accuracy of system information entered into CSAM fields, including control implementation statements, as part of continuous monitoring and in support of ongoing authorization throughout the system lifecycle.

***Control Overlay PL-02 ED-08 (L, M, H):*** Identify and document system authorization boundaries within the SSP in an accurate and consistent manner; the authorization boundary must:

a. Describe the information system's internal components and connections to external services and systems and include all federal data collected, stored, processed, generated, transmitted, or disseminated by the system.

b. Account for the flow of all federal information, data, and metadata through the system. Metadata identified should be accounted for, adequately protected, and documented within the System Security Plan (SSP), applicable system appendices and artifacts.

c. Illustrate the scope of control over the system as well as any system components or services that are leveraged from external systems or services.

d. Describe interconnections, Application Programming Interfaces (APIs), and other synchronous/asynchronous connections that are used to share federal data, metadata, and other information resources.

e. Development environments may be considered outside the authorization boundary if there is no federal information within this environment. If interconnections exist between the

development environment and the system's authorization boundary, they must be transparent and provided to the AO for review and risk acceptance.

f. Clearly delineate any external systems, components, and services used by the system which are not a part of the system and for which the system typically has no direct control over the application of required security and privacy controls or the assessment of security and privacy effectiveness. This shall be documented using Interconnection Security Agreements (ISAs) or Memorandum of Understandings (MOUs) and interconnection fields within CSAM.

g. Use of Managed Trusted Internet Protocol Service (MTIPS) for internet connectivity must be documented in ISA/MOU and CSAM.

h. Identify any corporate services such as customer relationship, ticketing, billing systems, etc. which are a subset of external services used by the system or used to support the system. If data that is being transmitted to these corporate services does not affect the confidentiality, integrity and availability of federal information, these services may be excluded from the authorization boundary; and

i. Provide a diagrammatic illustration of the system's internal services, components, and other devices along with connections to external services and systems.

## 2.3 PL-04 Rules of Behavior (P, L, M, H and Control Overlay)

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system.

c. Review and update the rules of behavior annually (i.e., each fiscal year).

d. Require individuals who have acknowledged a previous version of the Rules of Behavior to read and re-acknowledge when the rules are revised or updated.

***Control Overlay PL-04 ED-01 (L, M, H):*** Require network account holders to review and accept the Department's Rules of Behavior, *APPENDIX C: DEPARTMENT RULES OF BEHAVIOR*, in order to be marked as complete for initial and annual refresher (i.e., each fiscal year) Cybersecurity and Privacy Awareness training provided by OCIO.

***Control Overlay PL-04 ED-02 (L, M, H):*** Require the Principal Office to keep a record of Department network users who have accepted and acknowledged the Department's Rules of Behavior outside of the OCIO provided awareness and training program.

***Control Overlay PL-04 ED-03 (L, M, H):*** At a minimum, the rules of behavior for Department systems must:

a. Inform users of their responsibilities and accountability for their actions while accessing or administering a Department information system.

b. Define the consequences of noncompliance.

c. Inform users that they do not have any right to, or expectation of, privacy while using Department information systems, including internet and email services.

d. Require users to accept and acknowledge the rules of behavior before being allowed access to Department information systems

e. Include non-disclosure requirements when sensitive assets, information, and data is available for view.

### 2.3.1 PL-04(01) Rules of Behavior | Social Media and External Site/Application Usage Restrictions (P, L, M, H and Control Overlay)

Include in the rules of behavior, restrictions on:

a. Use of social media, social networking sites, and external sites/applications;

b. Posting organizational information on public websites; and

c. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

***Control Overlay PL-04(01) ED-01 (L, M, H):*** Social media restrictions defined in the Rules of Behavior shall comply with the ACSD-OCO-006[9], *Social Media Policy.*

## 2.4 PL-08 Security and Privacy Architectures (P, M, H and Control Overlay)

a. Develop security and privacy architectures for the system that:

    1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information.

    2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.

    3. Describe how the architectures are integrated into and support the enterprise architecture.

    4. Describe any assumptions about, and dependencies on, external systems and services.

[9] Also known as OCIO: 3-109.

b. Review and update the architectures at least annually (e.g., each fiscal year), and update as necessary, in conjunction with SSP reviews and updates to reflect changes in the enterprise architecture.

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

***Control Overlay PL-08 ED-01 (L, M, H):*** Use the current version of Department approved narrative templates to document system architectures using text and diagrams.

***Control Overlay PL-08 ED-02 (L, M, H):*** Incorporate CISA's Zero Trust Architecture (ZTA) maturity model, specifically the requirement for "advanced" maturity, into the Department's security architecture, and measure progress using information system continuous monitoring.

***Control Overlay PL-08 ED-03 (L, M, H):*** Include contractual security clauses in acquisitions which require third-party vendors/systems to identify and document current ZTA maturity and take actions required to achieve the ZTA maturity level required by the Department.

### 2.4.1 PL-08(01) Security and Privacy Architectures | Defense in Depth

Design the security and privacy architectures for the system using a defense-in-depth approach that:

a. Allocates multiple layers of security to information systems processing business sensitive information or are classified as an HVA; and

b. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

## 2.5 PL-09 Central Management (P)

Centrally manage planning, implementing, assessing, authorizing, and monitoring of common and hybrid (e.g., inherited) controls within the Department's enterprise CSAM tool.

## 2.6 PL-10 Baseline Selection (L, M, H and Control Overlay)

Select a control baseline for the system.

***Control Overlay PL-10 ED-01 (L, M, H):*** Select baseline controls from the current version of NIST Special Publication 800-53 in accordance with the information system security categorization.

## 2.7 PL-11 Baseline Tailoring (L, M, H and Control Overlay)

Tailor the selected control baseline by applying specified tailoring actions.

***Control Overlay PL-11 ED-01 (L, M, H):*** Tailor the initial control baseline to:

a. Include all control overlays required to implement Department specific policy requirements which are in addition to the controls contained within NIST 800-53.

b. Include the NIST 800-53 privacy baseline controls when the Privacy Threshold Analysis (PTA) determines the system collects, maintains, uses, or discloses personally identifiable information (PII).

c. Accept controls offered by Department programs and other systems as either common or hybrid. Clearly document as part of the SSP, the selection of system-specific security controls with traceability to the requirements and supporting rationale for any selection decisions made. Include sufficient detail in the description of security controls to be implemented to enable validation and assessment of the actual control implementation.

# 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 Directives |
| AO | Authorizing Official |
| API | Application Programming Interface |
| ATO | Authorization to Operate |
| BCP | Business Continuity Plan |
| BCPT | Business Continuity Plan Test |
| BIA | Business Impact Analysis |
| BOD | Binding Operational Directives |
| CIO | Chief Information Officer |
| CISA | Cybersecurity & Infrastructure Security Agency |
| CISO | Chief Information Security Officer |
| CM.AW-P | Data Processing Awareness |
| CMP | Configuration Management Plan |
| CM-P | Communicate-P |
| CPT | Contingency Plan Test |
| CSAM | Cyber Security Assessment and Management |
| CSF | Cybersecurity Framework |
| CSP | Cloud Service Provider |
| CT.DP-P | Disassociated Processing |
| CT.PO-P | Data Processing Policies, Processes, and Procedures |
| CT-P | Control-P |
| DE | Detect |
| DE.DP | Detection Processes |
| Department | U.S. Department of Education |
| DHS | U.S. Department of Homeland Security |
| DRP | Disaster Recovery Plan |
| DRPT | Disaster Recovery Plan Test |
| ED | U.S. Department of Education |
| EO | Executive Order |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act |
| FTRI | Federal Tax Return Information |
| GRP | Governance, Risk and Policy |
| H | High |
| HVA | High Value Assets |
| IA | Information Assurance |
| IAA | Inter-Agency Agreement |
| IAS | Information Assurance Services |
| ID | Identify |
| ID.AM | Asset Management |
| IRP | Incident Response Plan |
| IRPT | Incident Response Test Plan |

| Acronym | Definition |
|---|---|
| IRS | Internal Revenue Service |
| ISA | Interconnection Security Agreement |
| ISCP | Information System Contingency Plan |
| ISO | Information System Owner |
| ISSM | Information System Security Manager |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| L | Low |
| M | Moderate |
| MOU | Memorandum of Understanding |
| MTIPS | Managed Trusted Internet Protocol Service |
| NIST | National Institute of Standards and Technology |
| OCIO | Officer of the Chief Information Officer |
| ODP | Organizationally Defined Parameters |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| PF | Privacy Framework |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PIN | Personal Identification Number |
| PL | Planning Family |
| PR | Protect |
| PR.IP | Information Protection Processes and Procedures |
| PR.PO-P | Data Protection Policies, Processes, and Procedures |
| PR.PT | Protective Technology |
| PR.PT-P | Protective Technology |
| PR-P | Protect-P |
| PTA | Privacy Threshold Analysis |
| PUB | Publication |
| RAF | Risk Acceptance Form |
| SAOP | Senior Agency Official for Privacy |
| SAT | Security Assessment Team |
| SLA | Service Level Agreement |
| SP | Special Publication |
| SSP | System Security Plan |
| USB | Universal Serial Bus |
| User ID | User Identification |
| VPN | Virtual Private Network |
| ZTA | Zero Trust Architecture |

# 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 PF Category | CSF and PF Subcategory |
|---|---|---|---|---|---|---|---|
| PL-01 | Policy and Procedures | X | X | X | X | | |
| PL-02 | System Security and Privacy Plans | X | X | X | X | PR.IP, DE.DP, PR.PO-P | PR.IP-7, DE.DP-5, PR.PO-P5 |
| PL-04 | Rules of Behavior | X | X | X | X | | |
| PL-04(01) | Rules of Behavior \| Social Media and External Site/application Usage Restrictions | X | X | X | X | | |
| PL-07 | Concept of Operations | | | | | | |
| PL-08 | Security and Privacy Architectures | X | | X | X | ID.AM, PR.PT, CT.PO-P, CT.DP-P, CM.AW-P, PR.PT-P | ID.AM-3, PR.PT-5, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3, PR.PT-P4 |
| PL-08(01) | Security and Privacy Architectures \| Defense in Depth | | | | | ID.AM, PR.PT, CT.PO-P, CT.DP-P, CM.AW-P, PR.PT-P | ID.AM-3, PR.PT-5, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3, PR.PT-P4 |
| PL-08(02) | Security and Privacy Architectures \| Supplier Diversity | | | | | ID.AM, PR.PT, CT.PO-P, CT.DP-P, CM.AW-P, PR.PT-P | ID.AM-3, PR.PT-5, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3, PR.PT-P4 |
| PL-09 | Central Management | X | | | | | |
| PL-10 | Baseline Selection | | X | X | X | | |
| PL-11 | Baseline Tailoring | | X | X | X | | |

# APPENDIX B: REQUIRED NARRATIVES, APPENDICES, AND OTHER DOCUMENTATION

Principal Offices must use Department approved templates, available in the IAS Document Library within connectED or CSAM, to develop, implement, and maintain the following artifacts which support the SSP and are required to obtain and maintain an ATO. Upload the required documents into CSAM using the locations shown in the table below.

| CSAM Location | Document Type | Description | Review Frequency | Signature Requirement | Comments |
|---|---|---|---|---|---|
| Narratives | Technical Description | The completed narrative must describe technical characteristics of the information system including network architecture, data flow, and system ports, protocols, and services. | Annual | Covered by initial and annual CSAM-generated SSP signature; no separate signature required | Use of the ED technical description narrative template is not required for cloud service providers (CSPs) and Shared services |
| Narratives | System Description | The completed narrative must describe the functional and technical characteristics of the information system, including system function or purpose, system user types, system components and boundaries, and system environment description. | Annual | Covered by initial and annual CSAM-generated SSP signature; no separate signature required | Use of the ED system description narrative template is not required for CSPs and Shared Services |
| Appendix Q2; Status & Archive | Configuration Management Plan (CMP) | The completed CMP must satisfy NIST SP 800-53, Control CM-9 requirements and:<br>1. Address roles, responsibilities, and configuration management processes and procedures;<br>2. Establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the | Annual | Covered by initial and annual CSAM-generated SSP signature; no separate signature required | As per Control Overlay CM-9 ED-01, use of the ED CMP template is not required for CSPs and Shared Services |

| CSAM Location | Document Type | Description | Review Frequency | Signature Requirement | Comments |
|---|---|---|---|---|---|
| | | configuration items; and<br>3. Define the configuration items for the information system and places the configuration items under configuration management. | | | |
| Appendix L; Continuity & Incident Response | Information System Contingency Plan (ISCP) | The completed ISCP must satisfy NIST SP 800-53, Control CP-2 requirements and:<br>1. Identify essential missions, business functions, and associated contingency plan requirements;<br>2. Provide recovery objectives, restoration priorities, and metrics;<br>3. Address contingency roles, responsibilities, assigned individuals with contact information;<br>4. Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and<br>5. Address eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented. | Annual | ISO and ISSO | As per Control Overlay CP-2, ED-01, not required for CSPs and Shared Services |
| Continuity & Incident Response | Contingency Plan Test Results (CPT) | To satisfy NIST SP 800-53, Control CP-4, results of annual contingency plan testing completed must be documented in the current version of the ISCP (e.g., ISCP, Appendix K). | Annual | Covered by initial and annual ISCP signatures | As per Control Overlay CP-4 ED-01, CSPs and Shared Services are not required to upload artifacts in CSAM. However, testing dates must be |

| CSAM Location | Document Type | Description | Review Frequency | Signature Requirement | Comments |
|---|---|---|---|---|---|
| | | | | | entered into CSAM for all systems. |
| Appendix O; Continuity & Incident Response | Incident Response Plan (IRP) | The completed IRP must satisfy NIST SP 800-53, Control IR-8 requirements and:<br>1. Provide the organization with a roadmap for implementing its incident response capability;<br>2. Describe the structure and organization of the incident response capability;<br>3. Provide a high-level approach for how the incident response capability fits into the overall organization;<br>4. Meet the unique requirements of the organization, which relate to mission, size, structure, and functions;<br>5. Define reportable incidents;<br>6. Provide metrics for measuring the incident response capability within the organization;<br>7. Define the resources and management support needed to effectively maintain and mature an incident response capability. | Annual | Covered by initial and annual CSAM-generated SSP signature; no separate signature required | As per Control Overlay IR-8 ED-01, not required for CSPs and Shared Services |
| Appendix S | Hardware Listing | All system hardware within the authorization boundary is documented as required to satisfy NIST SP 800-53, Control CM-8. | Quarterly | Covered by initial and annual SSP signature; no separate signature required | As per CM-8, not required for CSPs and Shared Services |
| Appendix T | Software Listing | All system software within the authorization boundary is documented as required to satisfy NIST SP 800-53, Control CM-8. | Quarterly | Covered by initial and annual SSP signature; no separate | As per CM-8, not required for CSPs and Shared |

| CSAM Location | Document Type | Description | Review Frequency | Signature Requirement | Comments |
|---|---|---|---|---|---|
| | | | | signature required | Services |
| Appendix V2; Privacy | Privacy Threshold Analysis (PTA) | Required for all systems. | Every two years | ISO, Privacy Safeguards Division, and Senior Agency Official for Privacy (SAOP) | |
| Appendix V3; Privacy; System Identification | Privacy Impact Assessment (PIA), if required | Must be completed when the PTA shows that a PIA is necessary to comply with Department policy, OM 6-108, *Privacy: Section 208 of the E-Government Act of 2002 Policy and Compliance and* NIST SP 800-53, Control RA-8. | Every two years | ISSO, ISO, Privacy Safeguards Division, and Senior Agency Official for Privacy (SAOP) | Please consult the Department SAOP for CSPs and Shared Services |
| Relationships Section | Memoranda of Understanding (MOU), Interconnection Security Agreements (ISAs), Inter-Agency Agreements (IAA), and Service Level Agreements (SLAs) – if required | MOUs are required for when system(s) provide or receive controls from another system(s). To comply with NIST SP 800-53, Control AC-20, Use of External Information Systems and Department Directive OPEPD 1-101, *Interagency Agreements,* terms and conditions must be established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access an information system from external information systems; and process, store, or transmit organization-controlled information using external information systems. Principal Offices must complete the current version of the Department's approved template for Inter Agency Agreements (IAA) or Interconnection Security | Annual | Based upon connection type and Department template | |

| CSAM Location | Document Type | Description | Review Frequency | Signature Requirement | Comments |
|---|---|---|---|---|---|
| | | Agreements (ISA) to establish and approve these terms and conditions.<br>Completed MOUs, IAAs , ISAs, and SLAs must be uploaded into CSAM (if applicable). | | | |
| Appendix W; Continuity & Incident Response | Business Impact Analysis (BIA) | The completed BIA must:<br>1. Determine mission/business processes and recovery criticality along with outage impacts, estimated downtime, and recovery time objectives;<br>2. Identify resource requirements including facilities, personnel, equipment, software, data files, system components, and vital records and;<br>3. Identify recovery priorities for system resources. | Annual | ISO and ISSO | As per Control Overlay CP-2, ED-01, not required for CSPs and Shared Services |
| Status & Archive and Appendix CL: SSP Review Checklist | SSP Checklist | The completed SSP Checklist documents reviews performed to ensure system security information is accurate, thorough, and timely. | Annual | ISO and ISSO | As per Control Overlay PL-2 ED-03, not required for CSPs, Shared Services or OIG |
| Continuity & Incident Response | Incident Response Plan Test Results (IRPT) | Results of annual incident response plan testing are documented as required to satisfy NIST SP 800-53, Control IR-3. | Annual | Covered by initial and annual IRP signatures | As per Control Overlay IR-3 ED-01,CSPs and Shared Services are not required to upload artifacts in CSAM; however, testing dates must be entered into CSAM for all systems |

| CSAM Location | Document Type | Description | Review Frequency | Signature Requirement | Comments |
|---|---|---|---|---|---|
| Appendix P; Status & Archive | Disaster Recovery Plan (DRP) | Completed DRP establishes comprehensive procedures to restore operability of the system quickly and effectively at an alternate site in the event of a major hardware or software failure or destruction of facilities. | Annual | ISO and ISSO | As per Control Overlay CP-2 ED-02, not required for CSPs, Shared Services, subsystems and Low FIPS 199 categorized systems |
| Appendix P; Status & Archive | DRP Test | Result of annual disaster recovery plan testing completed and must be documented. For new systems, ensure system is stable in production for a period of no less than six months before performing DRP testing with DRP testing completed no later than one year from the initial ATO. | Annual | ISO and ISSO | As per Control Overlay CP-4 ED-02, not required for CSPs, Shared Services, subsystems or Low FIPS 199 categorized systems. |
| Appendix L2 | Business Continuity Plan (BCP) | Completed Principal Office BCPs satisfy NIST SP 800-53 Control CP 2(3) requirements and are uploaded to the PO specific program in CSAM. | Annual | | Only required for Principal Office Programs |
| Appendix L3 | Business Continuity Plan Test (BCPT) | BCPT results are documented as required to satisfy NIST SP 800-53 Control CP 2(3) and uploaded to the PO specific program in CSAM. | Annual | | Only required for Principal Office Programs |

# APPENDIX C: DEPARTMENT RULES OF BEHAVIOR

**U.S. Department of Education**
**Information Technology (IT) System Rules of Behavior**

All Government and Contractor personnel of the Department of Education (ED) must follow the rules of behavior set forth in this document when accessing and using IT equipment, systems, and departmental data and information. The Department of Education computer network provides access to e-mail, the Internet, Intranet, and most other systems required for the execution of the Department's mission. All personnel authorized access will be held accountable for their actions. Violations of the rules of behavior will be brought to the attention of Management for action, as situations warrant (e.g., personnel found in violation may face disciplinary action). According to the Department's Handbook for Information Assurance (IA) Security Policy, personnel who violate the rules may have their access to the ED computer network revoked. The rules described below are not to be used in place of existing policy, rather they are intended to enhance and define the specific rules each user must follow while accessing the Department of Education computer network.

This applies to all Government and Contractor personnel who have access to Department of Education computer network systems, data, records, and files. Further, all Government and Contractor personnel must adhere to all Department of Education Policy, Guidance and Procedures which include, but are not limited to:

- You are prohibited from uploading offensive or objectionable material to, or downloading from, the Internet. Refer to ACSD-OCIO-008[10], "Personal Use of Government Equipment and Information Resources", dated April 10, 2019;
- You must not knowingly, and with the intent to defraud the U.S. Government, access a protected computer without authorization, or beyond your authorization level;
- You are prohibited from using the Department of Education computer network or computer equipment to engage in any activity that is illegal or otherwise expressly prohibited (e.g., political activity, lobbying activity prohibited by law or running a personal business). You are, however, permitted occasional personal use, provided that such use incurs only a negligible additional expense to the Department of Education; does not impede your ability to do your job, does not impede other employees' ability to do their jobs; occurs during off-duty hours, whenever possible; and is not for the purpose of generating income for yourself or anyone else;
- All computer resources (including personal computers, laptops, wireless devices, all parts of the Department of Education computer network, communication lines and computing

[10] Also known as OCIO: 1-104, dated April 10, 2006.

facilities) are to be used in accordance with ED ACSD-OCIO-008[11], "Personal Use of Government Equipment and Information Resources", policy;

- Be aware that all Department of Education network and system resources used and accessed by Government and Contractor personnel are subject to periodic test, review, audit, and monitoring;
- You must adhere to all Department of Education IT security policies, practices and procedures, as well as relevant Presidential Directives and Office of Management and Budget (OMB) memoranda;
- You must adhere to the handling and disclosure of information as set forth in the Freedom of Information Act and the Privacy Act;
- The confidentiality and integrity of information must be maintained. Therefore, information in any form shall be appropriately protected. You must not maliciously delete, modify, destroy or otherwise misuse any Department data or information; and
- You must complete the OCIO Annual Security Awareness Training, and, if you are identified as being key IA or IT personnel, you must complete the required annual specialized education and training requirements defined by the OCIO IAS organization.

**User IDs and Passwords**

All Government and Contractor personnel must adhere to the policy set forth in the Department of Education's IT Password Guidance, which includes, but is not limited to:

- You are prohibited from sharing your account information with anyone, and must take the appropriate action to ensure your account information is stored in a secure manner;
- Your password must be a mix of at least 12 characters that contain upper and lower case letters, two numbers and at least one special character;
- Passwords cannot resemble any part of your user-ID or name;
- Passwords cannot not be reused for 24 iterations;
- Passwords must be changed at least once every 90 days;
- If your User Identification (User ID) or password is compromised, you must report it immediately to your supervisor and ISSO/ Information System Security Manager (ISSM); and
- Personal Identification Numbers (PINs) will be constructed as required, by the token issuer of any system requiring a PIN for access.

[11] Also known as OCIO: 1-104.

**Account Inactivity**

The Department will implement procedures and methodologies to ensure adequate management of information system accounts.

- After 30 days of inactivity, the account shall be put in suspension within 5 working days and will be terminated after 90 days. If you will not access your account for 90 days, contact your ISSO in advance to avoid having your account terminated; and
- Accounts with a cyclical business model (normally not accessed within 30 days) will not be suspended after 30 days of inactivity. These accounts will be suspended after 30 days of inactivity of their normal access period. Example: if an account with a cyclical business model is only accessed every 60 days, then it would be suspended after 90 days of inactivity. These accounts should be coordinated through ISSO channels.

**Access to Information Must be Controlled**

- All Government and Contractor personnel will be given access to information based on a need to know. Bypassing web filtering is a violation of Department policy that can expose the user and the Department to risks;
- You must work within the confines of the access allowed, and you must not attempt to access information for which you do not have a need to know;
- Do not leave computers logged on and unattended. Log off at the end of each session, or use access control software (i.e., screen saver with password) or configure auto-lock for unattended use;
- All wireless devices must be password protected;
- Do not leave mobile, wireless devices or cell phones unattended. Handheld devices should be stored securely when left unattended. To prevent theft, make sure that add-on modules and accessories are adequately protected when not in use;
- You are prohibited from sharing mobile or wireless devices, cell phones, or calling cards that have been assigned to you;
- You are prohibited from using a dial-up modem to directly access the internal network or any internal network devices. Dial-up access to the networks must be through OCIO operated access servers, and will only be assigned to authorized personnel;
- Connection to the Internet shall be in accordance with the ED IA Security Policy;
- Users shall not establish Internet or other external network connections (e.g., via modem access or unauthorized virtual privacy network [VPN]) that could allow unauthorized non-Department of Education personnel to bypass security features, and gain access to Department systems and information;

- Users shall not connect unauthorized devices to any Department networks, systems or devices; and
- Users shall not access or attempt to access network resources, systems or devices with unauthorized devices.

**Proper Use of IT Resources**

- You are only authorized to access and use Department of Education licensed/approved software. The use of unlicensed software is strictly prohibited;
- All licensed/approved software and documentation must be used in accordance with the copyrighted license agreement;
- You are only authorized to back-up your data to a network device or approved backup device. You are prohibited from storing sensitive or mission-critical data on your systems' hard drive or handheld device;
- All Department of Education system resources, including hardware, software programs, files, paper reports, and data are the sole property of the Department of Education, and there should be no expectation of privacy;
- You are only authorized to use Department-approved universal serial bus (USB) drives; and
- Department-issued laptops should be physically secured with laptop locks in the workspace.

**Service Provisions and Restoration**

- The Department of Education Network will be available for use by authorized users, at a minimum, during core business hours; and
- The proper controls are in place to ensure the restoration of critical information systems in the event that the Department of Education Network becomes inoperable.

**Warning Banners**

All Government and Contractor personnel who request access to the Department of Education's computer network or systems must read, agree to, and adhere to the Department's Warning Banner before being granted access.

**Standard Mandatory Warning Banner**

- "You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only;

- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties; and
- By using this information system, you understand and consent to the following:
    - You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may monitor, intercept, search and seize any communication or data transmitting or stored on this information system; and
    - Any communications or data transiting by or stored on this information system may be disclosed or used for any purpose."

**Remote Log on Mandatory Warning Banner/User Agreement**

- You are accessing a U.S. Government information system, which includes this computer session, this computer network, and all computers connected to this network session;
- This information system is provided for U.S. Government authorized use only;
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties;
- Personnel using remote access shall not download or store Government information on private equipment, optical or digital media;
- By using this information system, you understand and consent to the following:
    - You have no reasonable expectation of privacy regarding any communications of data transiting this information system. At any time, the Government may monitor, intercept, search, and seize any communications or data transiting this information system; and
    - Any communications or data transiting this information system may be disclosed or used for any purpose.
- By logging on, I agree and consent to these terms and conditions.

**Acknowledgement**

I acknowledge that I have received as well as understand my responsibilities and will comply with the Rules of Behavior for access to Department IT systems, networks and information. I acknowledge that I have received as well as understand my responsibilities and will comply with the Rules of Behavior for access to Department IT systems, networks and information. I acknowledge my responsibility to conform to the above terms and conditions set forth by the Information Assurance Program on behalf of the Department of Education. I understand that my failure to sign this Rules of Behavior will result in the denial of access to Department systems, networks and information.