NEW YORK STATE EDUCATION DEPARTMENT'S

DATA PRIVACY AND SECURITY POLICY

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

The New York State Education Department (SED) has the responsibility for developing and implementing an effective data privacy and information security program. This policy document is a critical component of the program as it outlines the minimum requirements necessary to ensure the confidentiality, integrity, and availability of SED Information Technology (IT) assets and data. This includes all SED information systems and communication networks, whether owned, leased or rented by SED, and the information stored, processed, and transmitted on or by these systems and networks. This policy shall be published on SED's website.

1.2 OBJECTIVE

The objective of this policy is to address SED's responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its IT assets and data. In addition, these policies ensure SED 's adherence to applicable legal and regulatory requirements and conform to best practices across the entire data and IT system lifecycle of creation, collection, retention, dissemination, protection, and destruction.

1.3 SCOPE

This policy document applies to all SED employees, interns, volunteers, consultants, and third parties who receive or have access to SED IT assets or data.

1.4 OVERSIGHT

SED's Chief Privacy Officer shall annually report to the Board of Regents on data privacy and security activities, the number and disposition of reported breaches, if any, and a summary of any complaints submitted pursuant to Education Law §2-d. While this policy falls under the program purview of the Chief Privacy Officer, it is the product of the collaborative efforts and expertise of the Chief Privacy Officer, Chief Information Officer and Chief Information Security Officer and their staff.

1.5 DOCUMENT STRUCTURE

This document is organized as follows:

- Section 1 is the introduction and introduces the policies, outlines the purpose, and establishes the implementation applicability.

- Section 2 defines the roles and responsibilities for individuals tasked to oversee and manage the SED data privacy and information security program.
- Sections 3-10 provide a comprehensive set of privacy and cybersecurity policy statements. The policy statements are organized by function and include privacy and governance, asset management, access control, awareness and training, data security, information protection, maintenance, and anomalies and events. The headings align to SED's chosen cybersecurity framework – the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) categories. Where applicable, NIST CSF categories were merged and additional requirements added to better align to the SED organization and mission.

2 ROLES AND RESPONSIBILITIES

SED has established and appointed applicable roles with the mission to coordinate, develop, implement, and maintain the data privacy and information security program. The roles listed below identify these positions and the specific activities personnel are responsible for executing. The Chief Privacy Officer, CIO and CISO must work with their respective governance boards and external partners to implement and maintain policies that protect the confidentiality, integrity and accessibility of SED IT systems and data.

- The Chief Privacy Officer (CPO) is responsible for establishing the protection framework for managing data privacy risk and the risk of the loss of confidentiality and integrity of SED data, and managing the collection, use and disclosure of personal information by establishing policies, procedures, and practices in accordance with applicable laws, rules, regulations, SED policies, and recommended industry practices. The Chief Privacy Officer will coordinate the implementation of a data governance strategy and lead SED's Data Privacy Governance Board as part of that framework. Data privacy and protection activities must be integrated into SED's management activities, including strategic planning, capital planning, and system design and architecture.
- The Chief Information Officer (CIO) is responsible for ensuring that information technology systems, programs, and the data they utilize, process and store are secure and protected from unauthorized access, alteration, damage, or release to or access by unauthorized persons.
- The Chief Information Security Officer (CISO) is responsible for establishing the information security governance framework and overseeing SED's implementation of information security. Information security activities must be integrated into other management activities of the enterprise, including strategic planning, capital planning, and enterprise architecture.

The Information Security Committee, led by the CISO, with leadership representation from across SED must meet regularly to discuss the information security program, requirements, and risks concerns, as outlined in the Information Security Committee Charter.

- The Deputy Commissioners are responsible for implementing privacy and security policies and practices into the operations of their program offices and the Department, including strategic planning, budget planning, and organization architecture.

3 GOVERNANCE

SED shall develop, implement and maintain an organization-wide privacy and security program to address the confidentiality, integrity and accessibility of SED IT systems and data that support the operations and assets of SED, including those provided or managed by another organization, contractor, or other source.

3.1 ACCEPTABLE USE POLICY, USER ACCOUNT PASSWORD POLICY AND OTHER RELATED DEPARTMENT POLICIES

- Users must comply with NYSED's Information Security Policy, which outlines the responsibilities of all users of SED information systems to maintain the security of the systems and to safeguard the confidentiality of SED information.
- Users must comply with the Acceptable Use of IT Resources Policy in using Department resources.
- Users must comply with the User Account Password Policy.
- All remote connections must be made through managed points-of-entry in accordance with the Data Privacy and Security Guidelines for Remote Work and Telecommuting Policy.

3.2 DATA PRIVACY

- The confidentiality of SED data must be protected and must only be used in accordance with state and federal laws, rules and regulations, and SED policies to prevent unauthorized use and/or disclosure.
- SED's Chief Privacy Officer leads the Data Privacy Governance Board. The Data Privacy Governance Board reviews approves and/or provides guidance to SED program offices when the collection, disclosure, or new processing of personal information protected by law is contemplated.
- Where required by law, personal information, personally identifiable information, shall only be disclosed to third parties pursuant to a written agreement that includes terms and conditions necessary to protect such information.
- It is SED's policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes.

3.3 PRIVACY AND SECURITY RISK MANAGEMENT STRATEGY

- SED will have policies and practices in place that identify the risks to the confidentiality, integrity, and accessibility of its IT systems and data, and manage its operations and the actions of its employees and vendors to minimize, mitigate or eliminate identified risk in line with applicable laws, rules and regulations, and industry recommended practices. To aid implementation of this strategy, SED shall:
- Conduct routine penetration tests to identify vulnerabilities that could be exploited by adversaries.
- Develop policies, processes, and procedures to manage and monitor SED's compliance with regulatory, legislative, technical, and organization mandates that protect the confidentiality, integrity, and availability of data.
- Address data privacy requirements and compliance by third-party vendors through its contracting process and must include terms and provisions in its contracts that address the risks to SED IT systems and data.
- Adopt policies and processes to ensure risks to data are identified, assessed, and responded to timely. Establish a process to ensure that applicable policies and procedures that address the protection of data are reviewed for improvements and updates/changes in regulations annually.
- The risk management strategy must be implemented consistently across SED, and must be periodically reviewed and updated, as required, to address organizational changes.

3.4 PRIVACY AND SECURITY RISK ASSESSMENTS

- Whenever there is a significant change to SED's information system or environment of operation, when new systems are implemented, when major modifications are undertaken, when changes in data elements occur, or when a system is migrating or deployed to a third party or to the cloud, SED will perform a risk assessment that assesses impact on privacy of personal information and impact to data security to assess the risk to the privacy of personal information of such changes.
- The risk assessment must capture the data flow (e.g., where the data is coming from, where it is processed/stored, and whom it is shared with). In addition, the risk assessment must state the legal authority for the collection of the data, and records retention schedule covering how long the data must be stored in the information system.
- Risk assessment results must be formally documented and disseminated to appropriate personnel including the system owner, the CIO, CPO, CISO, and other SED stakeholders, as applicable.

4 ASSET MANAGEMENT

SED IT assets deemed critical for SED to achieve its mission and objectives must be identified and managed commensurate with their risk level and importance to the organization.

4.1 PHYSICAL DEVICE INVENTORY (HARDWARE)

- All physical information systems within SED shall be inventoried, and essential information systems identified in accordance with SED's Data Classification Policy.

4.2 SOFTWARE AND APPLICATIONS

- All software platforms and applications within SED shall be inventoried.
- Inventories must include detailed information about the installed software, including the version number and patch level.
- The software/application inventory must be updated periodically, using an automated process where feasible.

4.3 DATA FLOW MAPPING

- An inventory of the types of restricted and confidential data that SED collects, where it is stored, and the third parties that receive it or receive access to it must be maintained. The inventory must document the type of restricted or confidential data collected, the authorization and purpose of collection and external parties to whom it is disclosed, and the authorization and purpose for such disclosure.

5 ACCESS CONTROL

- Access controls shall be implemented on all SED physical and virtual information systems and assets maintained by SED or on behalf of SED, to protect against unauthorized information alteration, loss, denial of service, or disclosure, as outlined in the information security policy.
- SED must establish processes and procedures to ensure that data is protected and only those with a need to know or need to access to perform their duties and/or administrative functions can access the data. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with SED's mission and business functions.

- These duties and/or administrative functions must be captured in the risk assessment for each respective information system that collects, maintains, uses, and/or shares personal information.
- Where technically feasible, users must be provided with the minimum privileges necessary to perform their job duties.

6 AWARENESS AND TRAINING

All SED personnel, volunteers, interns, and contractors with access to SED information systems and/or information must complete data privacy and security awareness training on an annual basis.

7 DATA SECURITY

To protect the confidentiality, integrity, and availability of SED data residing within SED systems, data security and data privacy controls must be incorporated into all aspects of the information systems, including the communications among and with these systems, and with systems external to SED boundaries.

7.1 DATA IN TRANSIT AND AT REST

- All data in transit and at rest containing confidential or restricted information must be encrypted in accordance with the SED Encryption Standard, where technically feasible. Where encryption is not technically feasible, one or more approved compensating control(s) must be adopted that addresses the same risk in accordance with applicable policies, laws, regulations, and standards.
- Systems must implement cryptographic mechanisms to prevent unauthorized disclosure of data and detect changes to data during transmission where technically feasible, unless otherwise protected by appropriate safeguards.
- All SED laptop computers must be secured in accordance with the SED Encryption Standard.
- Removable media must not be used to store confidential or restricted information unless the removable media are encrypted in accordance with the SED Encryption Standard.
- Removable media that is written to must be encrypted in accordance with the SED Encryption Standard.

8 INFORMATION PROTECTION

System protection controls must be established, implemented, and enforced on all essential SED information systems in accordance with SED security standards.

8.1 CONFIGURATION MANAGEMENT

- An enterprise configuration management plan must be developed, documented, and implemented.
- Personnel with configuration management responsibilities must be trained on SED's configuration management process.
- A current baseline configuration of essential systems must be developed, documented, and maintained.
    - Baseline configurations for SED workstations and laptops must be established, and images must be automatically deployed.
    - Server implementations must be deployed from a common baseline image per operating system. Baseline configurations must be reviewed and updated as part of system component installations and upgrades.
- Previous versions of the baseline configuration must be retained to support rollback.

8.2 CHANGE CONTROL

- Proposed system changes must be reviewed and approved prior to implementation. No scheduled changes are permitted outside of the configuration management process. The results of security impact analyses must be considered as part of the change approval process.
- Changes to systems (to include security patches) must be prioritized and implemented in a manner that ensures maximum protection against IT security vulnerabilities and minimal impact on business operations.
- If required changes (to include patches) are not applied, an approved risk-based decision must be documented.
- Approved changes (to include patches) must be tested and validated on non-production systems prior to implementation, where technically feasible. System changes must be analyzed to determine potential security impacts prior to change implementation.

8.3 BACKUPS

- Backups of critical SED systems and data must be conducted. The strategy to support system and data recovery must be documented.
- Backup data to be used for disaster recovery efforts must be stored at a secure off-site location.
- The confidentiality, integrity, and availability of backup information must be protected.
- Recovery procedures must be tested at least annually to verify procedure validity, media reliability, and information integrity. The result of the testing must be documented.

8.4 PHYSICAL ENVIRONMENT

- Controls must be implemented to ensure the physical and environmental protection of data and systems.
- Such controls must be commensurate with the level of data being stored, transmitted or processed in the physical location but can include emergency power shutoff, standby power, fire detection/suppression systems, environmental controls and monitoring, and physical access control and monitoring.

8.5 DATA SANITIZATION

- All sanitization and disposal techniques must be performed in accordance with SED's Secure Disposal Standard.
- All media sanitizations must be tracked, documented, and verified.
- Sanitization procedures must be tested.
- Both electronic and hard copy media must be sanitized prior to disposal, transfer, release out of organizational control, donation, or release for reuse, using sanitization techniques and procedures as outlined in the Secure Disposal Standard.
- Personal identifiers must be removed from personal information to make it anonymous before it is provided to third parties who require it for research or before it is published publicly such that the data cannot be used to identify a specific individual.

8.6 RESPONSE PLANNING

- SED's CISO, CIO and CPO have developed an Incident Response Policy and Plan to guide its response to data and cybersecurity incidents. The Incident Response Policy must be employed when an incident occurs.
- The Incident Response Plan must be:
    - Reviewed at least annually and updated to address system/organization changes.
    - Communicated to staff with incident response responsibilities.
    - Protected from unauthorized disclosure or modification.

8.7 VULNERABILITY MANAGEMENT

- A vulnerability management plan for SED systems and information processing environments must be developed and implemented. Systems must be scanned for vulnerabilities and vulnerabilities must be remediated in accordance with an assessment of risk within maximum allowable timeframes.

9 MAINTENANCE

Repairs and maintenance on all hardware and software must be controlled and performed only by approved personnel. Questions about approval will be addressed by the Chief Information Officer. Security commensurate with the sensitivity level of the system data must be implemented to protect data and information systems from unauthorized access or modification.

- All maintenance activities must be approved and monitored by designated system/facility staff.
- To the extent possible, all maintenance activities must be scheduled in advance and approval granted by the impacted parties.
- All software patches and updates must only be deployed after research and testing has been conducted in a development or test environment, where such test or development environments exist. Unless no test or development environment exists, software patch and/or update testing on operational systems is prohibited.
- All systems must be reviewed on a regular basis to ensure that current patches are applied.
- Maintenance tools must be inspected, approved, controlled, and monitored. All media must be checked for malicious code before being introduced to the production environment.
- A process for maintenance personnel authorization must be established and a list of authorized maintenance organization/personnel must be maintained.
- Session and network connections for remote maintenance must be terminated when non-local maintenance is completed.
- Remote maintenance and diagnostic sessions must be audited, and the records reviewed by designated system/facility staff.

9.1 PROTECTION AND MONITORING

SED IT assets must be adequately protected, controlled, and monitored. Security protections commensurate with the sensitivity level of the system data must be implemented to protect SED IT assets from unauthorized access or modification.

9.2 AUDIT

- SED-designated audit logs must be recorded, retained, and available for analysis by authorized personnel to identify unauthorized activity.
- Access to the management of audit functionality must be restricted to authorized personnel only.
- Where technically feasible, audit records must be correlated across different repositories and sources to gain SED-wide situational awareness and enhance the ability to identify suspicious

activity.

- Internal system clocks must be used to generate time stamps for audit records.
- All audit logs must be protected from unauthorized modification, access, or destruction in accordance with the sensitivity of the data stored therein.
- Audit information and tools must be protected from deletion, unauthorized access, and modification.
- Audit logs must be retained for a minimum of 30 days, where technically feasible.
- Audit trails capable of automatically generating and storing security audit records must be implemented on multi-user systems.

9.3 MEDIA PROTECTION

- All information system media (e.g., disk drives, diskettes, internal and external hard drives, portable devices, etc.), including backup media, removable media, and media containing SED information and/or sensitive information must be secured and protected from unauthorized access at all times.
- Access to digital and non-digital media must be restricted to appropriate personnel.
- All media, including backup media, must be stored securely, and transmitted securely to an off-site location in accordance with applicable business continuity and disaster recovery procedures.
- System media must be physically controlled and securely stored until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

9.4 LEAST FUNCTIONALITY

- All IT systems must be configured to provide only essential capabilities.
- Servers must not be used as workstations.
- The use of high-risk functions, ports, protocols, and/or services must be prohibited or restricted, as appropriate.

9.5 COMMUNICATION PROTECTION

- Data privacy and security controls must be incorporated into all aspects of information system and communications, to protect the confidentiality, integrity, and availability of SED information systems, data residing within these systems, and the communications among and with these systems, and with systems external to SED.

10 ANOMALIES & EVENTS

- System controls and processes must be implemented to ensure system and data integrity (i.e., accuracy, completeness, validity, and authenticity of systems and data) is protected at all times. Measures must be taken to prevent, detect, remove, and report malicious code, viruses, worms, and Trojan horses.
- SED must monitor systems to detect events for indicators of potential attacks and attacks, and conduct security testing, training, and monitoring activities associated with SED information systems.
- Security incidents must be tracked and documented.

10.1 BREACH/INCIDENT RESPONSE PLAN

The Department will respond to data privacy and security incidents in accordance with its Incident Response Policy and Plan. The incident response process will determine if there is a breach.

- The Incident Response Policy and Plan establishes a data breach response process and creates an Incident Response Team (IRT) comprised of existing staff members to address data breaches. Together with the CISO, the IRT must assess the potential impact of the incident and develop and execute a response plan consistent with SED established procedures and requirements.
- Employees must report suspected cybersecurity incidents to the Information Security Office and their immediate supervisor or manager. If a critical incident is verified, the CISO must convene a meeting of the IRT and notify senior management.
- The IRT will notify the Chief Privacy Officer where personal, confidential or sensitive information has been accessed by or disclosed to an unauthorized person. Where a breach is confirmed, the CPO will notify senior management and coordinate the process of compliance with notification requirements. SED will comply with legal requirements that pertain to the notification of individuals affected by a breach or unauthorized disclosure of personally identifiable information.
- Communication with the media, executive branch and Board of Regents regarding an incident must be coordinated with the Office of Communications.

11 APPENDIX A: GLOSSARY

Assurance	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Record	An individual entry in an audit log related to an audited event.
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See *Authentication*.
Availability	Ensuring timely and reliable access to and use of information.
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
Confidential Information	Confidential Information is information that is prohibited from disclosure by law, rules, or regulations or by SED's policies. It includes personally identifiable information and personal information. Access to confidential information is limited to those SED representatives who need such information to carry out their duty. When confidential information is received from another office, the receiving office must accept the responsibility for the confidential information and secure it appropriately.
Confidentiality	Preserving authorized restrictions on data access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Department	The New York State Education Department. Also known as SED within this document.
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form.
Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See *Organization*.
Enterprise Architecture	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.
Environment of Operation	The physical surroundings in which an information system processes, stores, and transmits information.
Event	Any observable occurrence in an information system.
External Network	A network not controlled by SED.
Firmware	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

Hardware	The physical components of an information system. See *Software* and *Firmware*.
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information System Component	A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Internal Network	A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned yet may be organization-controlled while not being organization-owned.
Local Access	Access to an SED information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
Malicious Code **Malware**	Software or firmware intended to perform an unauthorized process that must have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Media	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Multifactor Authentication	Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Network Access	Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
Nonlocal Maintenance	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
Organization	An entity of any size, complexity, or positioning within an organizational structure (e.g., a state department or, as appropriate, any of its operational elements).
Organizational User	An SED employee or an individual SED deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to SED, and citizenship.
Personally Identifiable Information (PII) or Personal Information (PI)	Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
Public Information	Public Information is information accessible under the Freedom of Information Law and is available to any person, without regard for one's status or interest.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that SED and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Remote Access	Access to a SED information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
Remote Maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
Restricted Information	Restricted Information is information that is not public information but can be disclosed to or used by SED representatives to carry out their duties, so long as there is no legal bar to disclosure. Information may also be accessible to a person who is the subject of the information under the Personal Privacy Protection Law.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of data or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Sanitization	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Incident	See *Incident*.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.
Security Policy	A set of criteria for the provision of security services.
Security Requirement	A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.

Security Service	A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.
Security-Relevant Information	Any information within the information system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.
SED IT Assets	SED information systems and communication networks, whether owned, leased or rented by SED, and the information stored, processed, and produced on or by these systems and networks.
Software	Computer programs and associated data that may be dynamically written or modified during execution.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See *Information System*.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment	Formal description and evaluation of threat to an information system.
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
User	Individual authorized to access an information system.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Analysis	See *Vulnerability Assessment*.
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.