 <p>NEW YORK STATE EDUCATION DEPARTMENT Information Security Office 10 N. Hawk Street Albany, NY 12210</p>	NYSED ISO POLICY
	<p>Data Classification Policy</p> <p>No: SECP7 - V:7.0 (11/8/2022)</p>
Issued By: NYSED Chief Information Security Officer	Owner: NYSED Information Security Office

1.0 Purpose and Benefits of the Policy

The policy establishes the data classification process for protecting the confidentiality, integrity, and availability of all data the New York State Education Department (SED) produces or is the custodian of both public and internal, written, and electronic.

This policy will adopt and apply the National Institute Standards and Technology Cybersecurity Framework (NIST CSF), regarding the New York State Education Department data classification process. Data classification is the basis for identifying an initial baseline set of security controls for data, data systems, and evaluation of retention and disposition schedules.

2.0 Scope

This policy applies to all data or information that is created, collected, stored, processed or managed by SED, or SED business partners, through its entire life cycle (i.e., generation, use, storage, and disposition); in electronic or non-electronic formats.

3.0 Requirements

All data created or used in support of SED business operations are owned by SED, regardless of form or format.

All data must be assigned a classification level, per the NYSED Information Security Policy.

The data classification level should be based upon the potential impact on SED; should certain events occur which interferes with the data or data systems needed to accomplish its assigned mission, responsibilities, and asset protection. Data classification must be reviewed on an ongoing basis to ensure that it has the appropriate classification level.

SED has established three data classification levels for the potential impact on the Department or individuals in the event of a data breach of security. The levels are defined as public information, restricted information, and confidential information. Each office should review the impact levels and apply them within the context of their operational environment.

The data classification levels to be used are as follows:

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.

Restricted Information – Restricted Information pertains to information, which is not public information, but can be disclosed to or used by SED representatives to carry out their duties, and anything that is not protected by regulation or law.

Examples of Restricted Information may include but are not limited to:

- Operational information
- Personnel records
- Information security procedures
- Research
- Internal communications

Confidential Information – Confidential Information is information that is prohibited from disclosure by law. 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.

Examples of Confidential Information may include but are not limited to:

- Personally Identifiable Information (PII), such as name in combination with Social Security number (SSN) and/or financial account numbers
- Intellectual property, such as vendor or third-party copyrights, patents
- Passwords used for authenticating individuals
- Network architecture schematics

Table 1 shows the data classification impact level definitions used in NIST 800-60 Vol 2 based on data classification.

	Potential Impact¹		
	LOW	MODERATE	HIGH
Confidentiality² A loss of confidentiality is the unauthorized disclosure of information. Consider the adverse effect on data types such as: <ul style="list-style-type: none"> • SED Mission/Programs • Personally Identifiable Information (PII) • System security plans • Organization Reputation 	The unauthorized disclosure of information could be expected to have a limited or no adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity A loss of integrity is the unauthorized modification or destruction of information. Consider the adverse effect on data types such as: <ul style="list-style-type: none"> • SED Mission/Programs 	The unauthorized modification or destruction of information could be expected to have a limited or no adverse effect on	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on

¹ NIST SP 800-60 Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf

² FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems: <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

<ul style="list-style-type: none"> • Personally Identifiable Information (PII) • System security plans • Organization Reputation 	organizational operations, organizational assets, or individuals.	organizational operations, organizational assets, or individuals.	organizational operations, organizational assets, or individuals.
Availability A loss of availability is the disruption of access to or use of information or an information system. Consider the adverse effect on data types such as: <ul style="list-style-type: none"> • SED Mission/Programs • Personally Identifiable Information (PII) • System security plans • Organization Reputation 	The disruption of access to or use of information or an information system could be expected to have a limited or no adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

(Table 1)

Guidelines for Classification

The guidelines listed below must be evaluated by SED departments when assigning classification to their data assets.

1. *A written or electronic inventory of all SED data assets.*

- The inventory should be maintained and arranged by group or category. For a more efficient application of security controls a narrow grouping may be useful to assist with precise targeting of controls.
- An asset must be classified at the highest level necessary based upon the data elements (e.g., financial server, payroll spreadsheet).
- Any data that is reproduce, must also have the same classification as the original data set. If the confidentiality classification of data stored electronically cannot be determined than it must be classified as restricted information at a minimum.
- If multiple data assets have the potential to be merged together or resides in the same location (e.g., server), the classification must be of the higher classification.

2. *Laws and Regulations*

- Ensure that all local, state, and federal laws, regulations, policies and standards relating to the data is adhered to.
- Account for ethical and privacy considerations.
- Any questions relating to the relevancy of any laws, regulations, policies and standards should be directed to the Office of Counsel.

3. *Risk of loss of confidentiality, integrity, and availability*

- Information must be classified based upon its value, sensitivity, misused, consequences if lost, and any state or federal requirements.

4. *Data Sharing and Contractual Agreements*

- If an agreement states that the recipient in the Department may share the data; the subsequent recipients must adhere to the requirements of the original classification unless the data has been modified and warrants a different classification.

5. *All information assets must have an Information Owner.*

- The responsibility for the classification and control of an information asset must be at the manger or executive level who is ultimately responsible for the confidentiality, integrity and availability of that information.
- Information owners must assign a classification to data/assets they own or oversee. The classification should be done by group or category.

- c. Information owners must determine access privileges and maintain access security controls for data custodians based upon the individual's duties.
- d. Information custodians are individuals, groups, units, or departments responsible for implementing the security controls for the data assets based upon the classification level.

Data Classification Process

SED Business Offices are responsible for developing a data classification process within the scope of their responsibilities.

The classification of data must be determined by the potential impact (high, moderate, low) for each principle of security in the confidentiality, integrity, availability (CIA) model as reflected in Table 1. The business offices must develop a formal process for granting and revoking access to SED data. A risk assessment must be performed to inform and assist managers to determine the appropriate controls that will ensure the proper level of protection for the data.

Data owners should work with subject matter experts such as the Office of Counsel, the Privacy Office, or the Information Security Office in determining if existing laws, regulations or agreements; limit or regulate the collection, use or transfer of SED owned data.

Labeled information will assist SED personnel with the necessary guidance to provide a consistent and appropriate classification determination.

Data Encryption

All electronically stored or transmitted data classified as Confidential Information or Restricted Information shall be encrypted while it is either at rest or in transit, using an approved cryptographic algorithm. All media containing SED data assets must be stored and shared, in a manner consistent with its security classification.

All non-public Asymmetric cryptographic keys as well as the resources used to generate and store the cryptographic keys shall be considered Confidential Information.

As defined by the National Institute of Standards and Technology ISO/IEC 18033-3, the minimum recommended encryption key will be AES 128-bit or stronger.

Legal Review

SED program offices in partnership with the Office of Counsel shall coordinate a legal review of all SED data classification labels to ensure compliance with all local, state, and federal laws or regulations that regulate the use or access of the data asset.

4.0 Compliance

This policy shall take effect upon publication. The Information Security Office (ISO) shall review the policy at least once every year to ensure relevancy. To accomplish this assessment, the ISO may issue requests for information from other program office departments. The information garnered will be used to develop any reporting requirements as may be requested by the Department's Chief Privacy Officer, the Board of Regents, or Legislative entities.

Any violation of this policy may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

5.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

NEW YORK STATE EDUCATION DEPARTMENT

Information Security Office

Website: <http://atwork.nysed.gov/iso/>

Email: infosec@nysed.gov

6.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
7/24/2019	DRAFT	CISO
1/27/2020	Subcommittee Review	
4/21/2020	Information Security Committee Review	ISC
4/27/2020	Update compliance section, update classification levels, update data sharing agreement	CISO
5/19/2020	<p>Section 1 Purpose and Benefits of the Policy:</p> <ul style="list-style-type: none">• The phrase “apply the Federal Information Processing Standards (FIPS), the National Institute Standards and Technology (NIST) Special publications”, has been removed as these standards do not apply to the data classification policy <p>Section 2 Scope:</p> <ul style="list-style-type: none">• The sentence “This policy applies to all SED employees, whether permanent or non-permanent, full or part-time, contractors, consultants, vendors, and business partners, who have access to or manage SED data”, has been removed to simplify the scope and remove any potential ambiguity. <p>Section 3 Requirements:</p> <ul style="list-style-type: none">• Examples for Restricted and Confidential Information has been added.• The Note: “Prior to the external release of any information please consult with the SED’s Data Privacy and Security Policy”, has been removed.• The title “Required Considerations for Classification” has been changed to “Guidelines for Classification”<ul style="list-style-type: none">- Bullet 4. Title “Data Sharing Agreements and Contractual Requirements” has been changed to “Data Sharing and Contractual Agreements”, also removed the multiple contractual agreements types and highlighted “If an agreement states that the recipient in the Department may share the data; the subsequent recipients must adhere to the requirements of the original classification unless the data has been modified and warrants a different classification”	CISO

	Section 4 Compliance: • Updated the violation of the policy to be consistent with HR policies language	
8/11/2020	Update requirements language for consistency in regard to the term data classification	CISO
10/01/20	Original Standard Release	
11/8/2022	Updated address and version number	Information Security Office
11/8/2024	Scheduled policy review	

7.0 Related Documents

- NYSED Data Privacy and Security Policy
- NYSED Information Security Policy
- NIST SP 800-60 Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems: <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- New York State Information Classification Standard

NEW YORK STATE EDUCATION DEPARTMENT'S

DATA PRIVACY AND SECURITY POLICY

Table of Contents

1	INTRODUCTION	1
1.1	PURPOSE	1
1.2	OBJECTIVE	1
1.3	SCOPE	1
1.4	OVERSIGHT	1
1.5	DOCUMENT STRUCTURE	1
2	ROLES AND RESPONSIBILITIES	2
3	GOVERNANCE	3
3.1	ACCEPTABLE USE POLICY, USER ACCOUNT PASSWORD POLICY AND OTHER RELATED DEPARTMENT POLICIES	3
3.2	DATA PRIVACY	3
3.3	PRIVACY AND SECURITY RISK MANAGEMENT STRATEGY	4
3.4	PRIVACY AND SECURITY RISK ASSESSMENTS	4
4	ASSET MANAGEMENT	5
4.1	PHYSICAL DEVICE INVENTORY (HARDWARE)	5
4.2	SOFTWARE AND APPLICATIONS	5
4.3	DATA FLOW MAPPING	5
5	ACCESS CONTROL	5
6	AWARENESS AND TRAINING	6
7	DATA SECURITY	6
7.1	DATA IN TRANSIT AND AT REST	6
8	INFORMATION PROTECTION	6
8.1	CONFIGURATION MANAGEMENT	7
8.2	CHANGE CONTROL	7
8.3	BACKUPS	7
8.4	PHYSICAL ENVIRONMENT	8
8.5	DATA SANITIZATION	8
8.6	RESPONSE PLANNING	8
8.7	VULNERABILITY MANAGEMENT	8
9	MAINTENANCE	9
9.1	PROTECTION AND MONITORING	9
9.2	AUDIT	9
9.3	MEDIA PROTECTION	10
9.4	LEAST FUNCTIONALITY	10
9.5	COMMUNICATION PROTECTION	10
10	ANOMALIES & EVENTS	11
10.1	BREACH/INCIDENT RESPONSE PLAN	11
11	APPENDIX A: GLOSSARY	12

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 <i>Authentication</i> .
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 <i>Organization</i> .
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 <i>Software</i> and <i>Firmware</i> .
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	<p>A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.</p> <p>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.</p>

Information System Component	<p>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.</p>
Information Technology	<p>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 <i>information technology</i> includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.</p>
Integrity	<p>Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.</p>
Internal Network	<p>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.</p>
Local Access	<p>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.</p>
Malicious Code Malware	<p>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.</p>
Media	<p>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.</p>
Multifactor Authentication	<p>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).</p>

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 <i>limited</i> adverse effect (FIPS Publication 199 low); (ii) a <i>serious</i> adverse effect (FIPS Publication 199 moderate); or (iii) a <i>severe</i> or <i>catastrophic</i> 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	<p>Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.</p> <p>Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.</p>
Security	<p>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.</p>
Security Control	<p>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.</p>
Security Functionality	<p>The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.</p>
Security Functions	<p>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.</p>
Security Impact Analysis	<p>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.</p>
Security Incident	<p>See <i>Incident</i>.</p>
Security Plan	<p>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.</p> <p>See <i>System Security Plan</i> or <i>Information Security Program Plan</i>.</p>
Security Policy	<p>A set of criteria for the provision of security services.</p>
Security Requirement	<p>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.</p> <p>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.</p>


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	<i>See Information System.</i>
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.

 <p>NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 10 N. Hawk Street Albany, NY 12210</p>	<p>NYSED Cloud Implementation Policy</p>
	<p>Information Security Policy</p> <p>No: SECP12 - V:6.0: (Rev 09/23/2024)</p>
<p>Issued By: NYSED Chief Information Security Officer</p>	<p>Owner: NYSED Information Security Office</p>

1.0 Purpose

The New York State Education Department (Department) recognizes the value of cloud services to enhance service delivery and improve operations. Cloud services have begun and will continue to change the Department operations and affect the IT (Information Technology) environment and services. The goal of this policy is to facilitate diverse uses of the cloud, ensuring optimal levels of the Department technology services. Therefore, this policy will outline how cloud services will interact with the Department infrastructure and services while maintaining mandatory minimum data security requirements.

2.0 Scope

Understanding the risks, threats, and costs associated with securing the Department data is a shared responsibility of all employees, volunteers, interns, consultants, and third-party contractors (Users) of the Department technology.

All Users considering the use of cloud services now or in the future must review this policy and comply with its requirements.

This policy applies to any cloud services that contains any NYSED data. This includes, but is not limited to:

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)

Cloud Service Provider (CSP) under consideration must demonstrate the ability to comply with all relevant components of Appendix 1, [Ed Law 2-d](#), local, federal, State laws and regulations.

3.0 Policy Statement

All program offices must inform Information Technology Services (ITS) of all proposed uses of cloud services to ensure that proper security, legal, and operational measures are considered.

Program areas are required to inform ITS by submitting a request through the [project management portal](#). ITS will work with program areas to confirm that the implementation is feasible.

All program areas seeking to select or implement a cloud service must submit their projects through the [project management portal](#) in the initial planning stage. ITS technical teams will provide guidance on the use of cloud services. Depending on the scope, ITS will determine whether an information security review is needed, advise on alternative solution pathways, if relevant, and/or provide other guidance, as applicable. Engaging with ITS as early as possible improves the capacity to evaluate the chosen solution pathway to ensure that required information security and other Department requirements can be met.

When Program offices select a platform or partner, it is mandatory to confirm the availability of either a SOC 2 type 2 report or an impartial party assessment completed within the last year based on the risk assessment.

Program areas must also abide by any relevant technology policies that apply to their implementation. Regardless of the hosting site, program offices' applications are subject to requirements regarding security accreditation, as well as established and enforced service level agreements (SLAs). In addition, program offices must adhere to the [data privacy and security policy](#) and properly classify any data stored in the cloud.

3.1 IaaS

IaaS is commonly used to procure commoditized application hosting. IaaS is a type of cloud computing service that offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis. All program offices use of IaaS must be managed through ITS, therefore program areas must submit their implementation plan to ITS through the [project management portal](#) in the initial planning stage, to determine the best approach and ensure Information Security.

Program areas using IaaS are responsible for working with ITS to ensure that their use of IaaS cloud services adhere to the data privacy and security policy and properly classify any data stored in the cloud.

3.2 SaaS/PaaS

SaaS refers to the purchase and use of software services hosted by the service provider. This service allows users to connect to and use cloud-based apps over the Internet. The policy also addresses Platform as a Service (PaaS), which provides a platform for developing, running, and managing applications. All program offices use of SaaS or PaaS must be reviewed and approved by ITS prior to procurement and implementation. The Department program offices must submit their plans to leverage a SaaS or PaaS solution through the [project management portal](#) in the initial planning

stage. ITS will review critical aspects of the SaaS or PaaS solution including, but not limited to, the following:

- Authentication and authorization
- Platform and hosting model
- Logging and auditing
- Data requirements
 - o Classification
 - o Recovery
 - o Storage model
 - o Retention and deletion
 - o Application security
 - o Infrastructure security

4.0 Roles and Responsibilities

ITS, in collaboration with the Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO), is responsible for ensuring that the Department infrastructure, networks, and applications are cloud-ready, and procedures are in place for connecting to the cloud. This includes maintaining secure connections, addressing information security risks, maintaining network bandwidth, and expanding cloud offerings with selected vendors as deemed necessary. ITS is the resource for program areas planning IT projects of all types, particularly cloud-based services. Applicable CSP applications should adhere to applicable regulations and/or guidance.

5.0 Definitions of Key Terms

Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses

personally identifiable information; or an authorized user accesses personally identifiable information for an other than authorized purpose.

Cloud: Refers to a term used for global networks; originally used to reference the telephone network, now commonly used as a reference to the Internet.

Cloud Computing: The practice of using a network of remote servers hosted on the internet (In an External Site) to store, manage, and process data.

Cloud Computing Service: Is a service provided by a third party to offer fully managed easy scalable access to applications, resources, and services.

Cloud Infrastructure: Is the collection of hardware and components, such as servers, storage, network, and virtualization software needed to support a cloud computing model.

Cloud Service Provider (CSP): Refers to an entity that provides cloud-based services.

Cloud Computing Service Models:

- *Software as a Service (SaaS):* The cloud service provider's application runs on a cloud infrastructure and is accessible by the consumer online via a web interface or via a desktop application. The consumer has no control over the underlying hardware configuration.
- *Platform as a Service (PaaS):* The consumer of the cloud service deploys or installs onto the cloud infrastructure a consumer-created or acquired application. The application must use programming languages, libraries, services, and tools supported by the cloud service provider. The consumer has no control over the underlying hardware configuration, storage, network, operating system, or management layers.
- *Infrastructure as a Service (IaaS):* The consumer utilizes the cloud service provider's processing and storage facilities, their network, and other computing resources. The consumer can install and run any software, which may include operating systems and applications. While the consumer does not have any control over the underlying cloud infrastructure, it has control over operating systems, storage, and deployed applications.

Cloud Computing Deployment Models:

- *Private Cloud:* The cloud infrastructure is commissioned for exclusive use by a single organization. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Also, they may exist in or outside the country.
- *Community Cloud:* The cloud infrastructure is commissioned for exclusive use by a specific community/sector of consumers from organizations that have shared nature of work and obligations. It may be owned, managed, and operated by one or more of the organizations in

the community, a third party, or some combination of them, and it may exist on or off premises. Also, it may exist in or outside the country.

- *Public Cloud:* The cloud infrastructure is commissioned for open use by any organization. It may be owned, managed, and operated by a private or public organization or a combination of them. It exists on the premises of the cloud service provider.
- *Hybrid Cloud:* The cloud infrastructure in a composition of two or more different cloud infrastructures (private, community, or public) that remain separate entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., load balancing between clouds).

Data Classification: Data classification requires that data be categorized according to its confidentiality/sensitivity level and degree of impact to the Department should the data be disclosed, altered, or destroyed without authorization. The baseline security controls implemented to safeguard data are determined by its classification. Data is classified in accordance with the [Data Classification Policy](#).

Information Security Program: At a high-level, refers to the policies, processes, and tools necessary to prevent, detect, document and counter security threats to digital and non-digital data. In sum, a security program defines the framework required for maintaining desired security levels. This policy is a crucial element of the Information Security Program.

User: All Department employees, volunteers, interns, consultants, and third-party contractors.

6.0 Compliance

This policy shall take effect upon publication. The Information Security Office (ISO) shall review the policy at least every two years to ensure relevancy. To accomplish this assessment, the ISO may issue requests for data from other program office. The data garnered will be used to develop any reporting requirements as may be requested by the NYSED's Chief Information Officer, Chief Privacy Officer, the Board of Regents, or Legislative entities.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The Department will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

7.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

NEW YORK STATE EDUCATION DEPARTMENT

Information Security Office

Website: [Information Security Office Intranet Site](#)

Email: infosec@nysed.gov

8.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
11/22/2022	DRAFT	Information Security Office
3/21/2023	Reviewed by CPO	Chief Privacy Officer
1/29/2023	Updated Purpose, Scope, and Policy Statement	Information Security Office
11/27/2023	Updated definitions and links to policy	Information Security Office
12/05/2023	Reviewed by ITS management team	CPO, ITS, ISO
08/08/2024	Updated language and removed specific providers by name	Information Security Office
09/04/2024	Updated language and removed specific for StateRamp and FedRamp	ITS, CPO, CAU, ISO
09/23/2024	Updated language and formatting	Information Security Office

APPENDIX

APPENDIX 1-Contract Considerations for Cloud Service Agreements

Cloud Service Provider (CSP) under consideration must demonstrate the ability to comply with all relevant local, federal, and State laws and regulations, including [Ed Law 2-d](#).

The following must be addressed to all CSPs (Cloud Service Provider) under consideration for cloud services and must demonstrate their compliance with applicable security controls.

Adjustments can be made in accordance with the type and scope of the cloud service.

Data

At a minimum, they should adhere to the following, this includes, but not limited to:

1. Backup:

- a. In cases where backup is required, all agreements should establish service level agreements.
2. Service level agreements (SLAs) for the restoration process include recovery time objective (RTO) and recovery point objective (RPO), and the CSP must demonstrate its ability to meet that SLA, with penalties established for failure to meet SLA.
 - a. Where backup is required, confidential data and its backups must be encrypted in transit and at rest.

3. Data Retention:

- a. Where legal mandates for data retention apply, all agreements must establish terms for preservation, retention, filtering, and retrieval. The CSP must demonstrate its ability to meet the legally mandated requirements.
- b. Even where legal mandates do not apply, the CSP may not delete or remove Department data without express permission of the business office to do so.
4. **Business Continuity:** Where Business Continuity/Disaster Recovery (BC/DR) services are required, all agreements should establish terms for BC/DR, and the CSP must demonstrate its ability to fulfill the terms. CSP must provide policies and procedures that address data availability, disaster recovery, data backup and retention when requested.

IT Security

Cloud providers should be able to demonstrate compliance with current Ed Law 2-d and the Department Security Policies. At a minimum, they should adhere to the following:

1. **Encryption:** The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the CSP in question and approved by the NYSED Chief Information Security Officer.
2. **Incidents:**

- a. The CSP should immediately notify the Department of any breach or attempted security intrusion following discovery.
- b. Upon the Department request, the CSP must supply all logs (including operating system, DBMS/database, and application logs) for the affected host machine.
- c. The CSP should provide a documented incident response plan.

3. Reporting:

- a. The CSP should provide notification of any breach and/or attempted breach in accordance with Ed Law 2.d.
- b. Any history of security breaches or attempted breaches must be disclosed.

4. Risk Management and Compliance – The CSP should be audited by a certified, impartial third-party, ensuring implemented security controls have been developed and maintained.

- a. Demonstration that independent audit assurance and compliance have been performed at least annually.

5. Enhancements/Upgrades: The CSP should notify the customer of any changes to the system, such as changes made, such as enhancements and upgrades, which can impact on the security of the system.

Support

At a minimum, they should adhere to the following, but not limited to:

1. Identity and Access Management:

- a. Have in place and provide when requested policies and procedures that address data flow, data handling, and disposal.
- b. Access Control – Required access management policies, practices, and technologies to ensure proper authentication, authorization, auditable and role-based access.

2. Personnel Security:

- a. Screening practices of personnel
- b. Record and tracking of personnel separating from the organization
- c. Record of annual Privacy and Security Awareness Training

3. Monitoring:

- a. The CSP should provide information about monitoring methodology including tools and procedures.

4. Upgrades:

- a. The CSP should give notification of upgrades.
- b. The CSP should outline how testing of upgrades will be performed.

Compliance

1. Access Control

- a. Required identity and access management policies, practices, and technologies to ensure authorization, secure authentication, role-based access, auditable access, and timely access termination.

2. Asset Management

- a. Policies and procedures that address data inventory, data flow, data classification, data labeling, and data handling (including disposal).

3. Data Protection

- a. Application & Interface Security to ensure that applications and programming applications and interfaces are designed, developed, deployed, and tested in accordance with the System's standards and adhere to applicable legal, statutory, or regulatory compliance obligations.
- b. Required data protection policies and procedures, including, but not limited to, encryption, penetration testing, vulnerability management, malicious code execution and data management solutions employed to ensure controlled access to data, to secure data while at rest, in transit and in use.
- c. Documented baseline of security configurations implemented along with documentation that demonstrates annual testing of same.
- d. Required physical and logical architecture and configurations to safeguard against unauthorized access of, intentional, or unintentional alteration of IT resources.

4. Shared Responsibility Model


- a. Department Responsibilities:
 - i. Data Classification: The program office is responsible for classifying its data based on sensitivity, ensuring that confidential, sensitive, and regulated data is appropriately identified.
 - ii. Data Access Control: The program office is responsible for defining and enforcing access controls to ensure that only authorized personnel can access sensitive data.
 - iii. Data Encryption: The program office is responsible for encrypting data at rest and in transit, employing appropriate encryption mechanisms based on the sensitivity of the data.
 - iv. User Access Management: The program office is responsible for managing user accounts, including provisioning, deprovisioning, and access revocation when necessary.
 - v. Security Monitoring: The program office is responsible for monitoring the security of its cloud environment, detecting and responding to any suspicious activities or security breaches.
- b. CSP Responsibilities:
 - i. Physical Security: CSPs are responsible for securing the physical infrastructure, including data centers, network facilities, and hardware components.
 - ii. Network Security: CSPs are responsible for securing the cloud network infrastructure, ensuring proper segmentation, firewalls, and intrusion detection systems (IDS) are in place.
 - iii. Virtualization Security: CSPs are responsible for securing the virtualization layer, ensuring proper isolation and protection between different virtual machines and tenants.

- iv. Patch Management: CSPs are responsible for applying security patches and updates to the underlying cloud infrastructure and ensuring timely vulnerability management.
- v. Data Storage Security: CSPs are responsible for securing the storage infrastructure, implementing measures such as redundancy, data backups, and disaster recovery mechanisms.
- vi. Application Security: In the case of SaaS, CSPs are responsible for securing the application layer, including authentication, authorization, and secure coding practices.
- vii. Incident Response: CSPs are responsible for promptly responding to security incidents, providing incident management, and cooperating with the Department in incident investigations.

References

NYS Information Technology & Telecommunications. 2016. *Citywide Policy on Cloud*. Accessed October 7, 2022. <https://www.bidnet.com/bneattachments?/418632796.pdf>.

NYC Health+ Hospitals, 2017. *Enterprise Information Technology Services Information Security & Risk Management: Security Policy on Cloud Computing Services*. Accessed October 7, 2022. <https://ess.nychhc.org/uploads/Security-Policy-on-Cloud-Computing-Services.pdf>

 <p>NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 10 N.Hawk Street Albany, NY 12210</p>	NYSED ISO POLICY
	<p>Secure Disposal Standard</p> <p>No: SECS6 - V:5.0: (Rev 9/27/2022)</p>
Issued By: NYSED Chief Information Security Officer	Owner: NYSED Information Security Office

1.0 Purpose and Benefits of the Standard

Department information, whether stored on Department systems, electronic media devices, printed out, or sent to or held by another organization, may contain Personal, Private, or Sensitive Information (PPSI) or Personally Identifiable Information (PII). Information systems capture, process, and store information using a wide variety of media, including paper. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These forms of media may require special disposal to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality.

The benefit to the department will be the secure and efficient disposal of media containing sensitive Department information.

2.0 Scope

This standard applies to all individuals, including employees, consultants, vendors, and third parties, who are responsible for disposing of PPSI/PII or responsible for the sanitization of any related electronic storage media that harbors such information.

This standard addresses the secure disposal of paper and electronic storage and associated media, provided that the disposal does not conflict with any data retention policies, laws, or regulations.

It is the responsibility of all users of Department IT resources to read and understand this standard and conduct their sanitizing and disposal in accordance with these terms. In addition, users must read and understand the NYSED Information Security Policy and its associated standards.

3.0 Information Statement

As per the NYSED Information Security Policy and NYS Information Classification Standard, information must be properly managed from its creation, through authorized use, to proper disposal.

The Department must:

- Ensure that users and custodians of information are aware of its sensitivity and the basic requirements for media sanitization and secure disposal.
- Ensure that all workforce members, including property management and custodial staff, are made aware of the media sanitation and secure disposal process to establish proper accountability for all data.
- Ensure that confidential material is destroyed only by authorized and trained personnel, whether in-house or contracted, using methods outlined in this standard.

The Department may use service providers for destruction purposes provided that the information remains secure until the destruction is completed. The service providers must follow this standard. Managers and Supervisors must ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 or similar compensating control in the absence of a data classification standard.

There are many risks related to the disposal of storage media, including unauthorized release of sensitive and/or confidential information, potential violation of software agreements, and unauthorized disclosure of copyright or other intellectual property. For these reasons, the following controls must be followed.

Paper Media

All paper-based media should be properly disposed of when it is no longer necessary for business use.

- Only paper media classified as “Public” should be disposed of using the standard disposal method (i.e. these documents can be placed in a recycling bin).

The following controls apply to all paper documents unclassified, classified at a level more sensitive than public, or containing personal, private, or sensitive information (PPSI) or personally identifiable information (PII).

- Documents can be placed in a designated locked Confidential Recycling bin or shredded internally.
- Cross cut shredding, pulverizing, disintegration, or incineration are the acceptable methods of destroying documents.
- All new shredders obtained by the Department must be crosscut by shredders.
- A third-party document destruction service may be contracted for destroying quantities of paper documents.
- A “Certificate of Destruction” must be obtained from the third-party destruction service after this process.

Electronic Media

The sale, transfer, surplusage, or disposal of computers, computer peripherals, computer software, and other IT devices can create information security risks for the Department due to the storage media used in these devices.

The following controls are required for secure disposal of all electronic media.

- Prior to any sanitization process:
 - Ensure that all important data or configurations are backed up to another location.
 - Ensure that the electronic storage device is disconnected from the Department network. (This ensures only the intended device is sanitized.)
- All electronic storage devices to be disposed of must be returned to IT.

Standard Disposal

- Standard Disposal is the act of discarding media with no other sanitization considerations. This is the acceptable method to dispose of paper documents containing only public information.
- Standard Disposal is acceptable for optical media (CD's, DVD's, etc.) labeled as "Public" or with no sensitive information contained on them.
- Standard Disposal must not be used for the disposal of any Department electronic storage devices (thumb drives, USB drives, etc.). Electronic storage devices must never be placed in a garbage or recycle bin without applying additional sanitization actions.

Media Sanitization Methods—Clear, Purge, Destroy

Method	Description
Clear	<p>One method to sanitize media is to use software or hardware products to overwrite user-addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user-addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable, and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface.</p> <p>The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared</p>

Purge	<p>Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands.</p> <p>Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques.</p> <p>Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device</p>
	<p>flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).</p>
Destroy	<p>There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques.</p> <p><i>Disintegrate, Pulverize, Melt, and Incinerate.</i> These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.</p> <p><i>Shred.</i> Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media).</p> <p>The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the</p>

Table 5-1: Sanitization Methods
(from NIST 800-88, Rev. 1, Guidelines for Media Sanitization)

Sanitization Decision Process

The decision process is based on the confidentiality of the information, not the type of media. The Department chooses the type of sanitization to be used, and the type of sanitization is approved by the Information Owner and Information Steward. The technology used may vary by media type and by the technology available to the custodian, so long as the requirements of the sanitization type are met.

Disposal without sanitization should be considered only if information disclosure would have no impact on organizational mission, would not result in damage to organizational assets, and would not result in financial loss or harm to any individuals.

The security categorization of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. The key is to first think in terms of information confidentiality, then apply considerations based on media type.

The cost versus benefit of a sanitization process should be understood prior to a final decision. The Department can always increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk. For example, even though Clear or Purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options. The Department may not decrease the level of sanitization required.

Electronic Storage Device Destruction Process

If electronic storage devices are destroyed within the Department, the following requirements must be met:

- All electronic storage devices to be destroyed must be returned to IT for destruction.
- Hard drives returned to IT for destruction must be destroyed as soon as they are received by IT.
- If hard drives are not destroyed immediately, they must be labeled that they need destruction, and stored in a secure locked location.
- After hard drives have been destroyed they must be sent to a third-party destruction service for final drive shredding and recycling.
- IT must maintain a record of the destruction to document what media were destroyed, when, how they were destroyed, and the final disposition of the media.

Documenting the Secure Disposal of Media and Devices

- The disposal of media and electronic storage devices containing PPSI or PII shall be documented.
- No storage device may be sent to surplus, recycled, returned to manufacturer, or leave the Department for any other reason without either being sanitized or destroyed, and with the appropriate documentation completed. For example:
 - Desktop systems returned to manufacturers due to contracts need to have the hard drives sanitized prior to sending back to the manufacturer.
 - Servers cannot leave the Department with their hard drives. Server hard drives must be destroyed, and the process documented.
- The documentation must include the name of the person authorizing the disposal and the reason for disposal.
- The documentation must include the disposal method and include the date the disposal took place and a log of the device being disposed containing these items.

Disposal of Sanitized Equipment

- Once sanitized, electronic equipment must be disposed of or sent to surplus in an environmentally sound manner. This includes all hardware, including servers, desktops, laptops, network equipment, destroyed disks, external, and removable storage, etc.
- Electronic equipment being disposed of should never be put in a trash bin or dumpster.
- IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from NYSED's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Privacy Breach Reporting

- The Information Security Office (ISO) will review compliance to this standard and will report any misuse or improper disposal of PPSI or PII to the Chief Privacy Officer (CPO). In accordance with

the Data Privacy and Security Policy and regulations (e.g. NYS Technology Law, the NYS Personal Privacy Protection Law, among others), the ISO and CPO may also be required to notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination.

4.0 Compliance

This standard shall take effect upon publication. The Information Security Office (ISO) shall review the standard at least every two years to ensure relevancy. To accomplish this assessment, the ISO may issue requests for information from other program office departments. The information garnered will be used to develop any reporting requirements as may be requested by the Department Chief Privacy Officer, the Board of Regents, or Legislative entities.

Any violation of this standard may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this standard on a case-by-case basis and pursue recourse, as appropriate.

5.0 Definitions of Key Terms

Electronic Storage Device: Any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, USB drives, SD cards, etc.

Electronic Media: Any material on which electronic data may be stored, such as magnetic tape, magnetic disks, solid state storage devices, or optical discs.

Solid-State Storage Device: A type of computer storage media that is made from microchips. Solid-state media stores data electronically instead of magnetically, as spinning hard disk drives, or magnetic oxide tape do. Examples include thumb drives, memory sticks, SD cards, Solid-State Disks (SSD), etc.

Standard Disposal: The act of discarding media with no other sanitization considerations. Simply discarding the media. An example would be by placing paper documents in a recycling bin.

Clearing: A level of sanitization that renders media unreadable through normal means. Simple deletion of items would not suffice for clearing. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Overwriting cannot be used for media that is damaged or not writeable.

Purging: Purging is the removal of data from a system or storage device with the intent that the data cannot be reconstructed by any known technique. Purging typically consist of using specialized utilities that repeated overwrite data.

Destroying: Rendering media unusable. After media is destroyed, it cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including crushing, disintegration, incineration, pulverizing, shredding, and melting. Optical storage media, including CD, CD-RW, CD_R, CD-ROM, DVD, Blu-ray, and magneto-optic (MO) disks are typically destroyed.

6.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

NEW YORK STATE EDUCATION DEPARTMENT

Information Security Office

Website: <http://atwork.nysed.gov/iso/>


Email: infosec@nysed.gov

7.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
08/03/2017	DRAFT	CISO
3/12/2019	Updated ISO Office and phone number, updated information in Section 1, and 4	Marlowe Cochran, Chief Information Security Officer
8/9/2019	Reviewed, Update standard terms	ITS, CPO, CISO
11/25/2019	Updated Contact Information	Marlowe Cochran, Chief Information Security Officer
12/5/2019	Original Standard Release	Marlowe Cochran, Chief Information Security Officer
9/27/2022	Updated date, address, version, and 'Disposal of Sanitized Equipment' section	Information Security Office

8.0 Related Documents

- NYSED Information Security Policy
- NIST 800-88, Rev. 1, Guidelines for Media Sanitization
- Data Privacy and Security Policy
- NYS Information Classification Standard

 <p>NEW YORK STATE EDUCATION DEPARTMENT Information Security Office (ISO) 10 N. Hawk Street Albany, NY 12210</p>	NYSED ISO STANDARD
	<p>Secure Remote Access Standard</p> <p>SECS5 – V:5.0 (REV 11/8/2022)</p>
Issued By: NYSED Chief Information Security Officer	Owner: NYSED Information Security Office

1.0 Purpose and Benefits of the Standard

The purpose of this standard is to effectively document, manage, and control remote access to the NYSED (the Department) computer network, and to define the protection and security requirements that support remote access. It is necessary for the Department to ensure network security by limiting the risk of intrusion and/or unauthorized access.

The benefit to the Department will be an enhanced security of Departmental information through secure and proper use of all remote access resources.

2.0 Scope

This standard applies to all Department IT remote access resources and all users of such resources.

It is the responsibility of users to read and understand this standard and to conduct their activities in accordance with its terms. In addition, users must read and understand the NYSED Information Security Standard and its associated standards.

3.0 Information Statement

General Requirements

Remote access to the Department's network is subject to the following requirements:

- Remote access must be for Department business purposes only. Access will be limited to those resources and levels required for relevant business functions.
- Remote access to the Department's network is limited to within the United States. Any access required outside of the United States will require further approval by the Information Security Office.
- Remote users only have access to resources within the Department's network that they require.
- Remote access activity will be logged and monitored for suspicious activity.
- Remote access sessions must not last any longer than 24 hours.
- All changes to the configuration of infrastructure equipment that supports remote access must follow the applicable Department change management processes. If a formal change management process

doesn't exist, all changes to the configuration of infrastructure equipment that supports remote access must be well documented and securely stored.

- All remote access connections (e.g. circuits with Virtual Private Network (VPN) tunnels to other facilities) or connection types (e.g. laptops using VPNs) must be approved by the Information Security Office (ISO), via the Secure Remote Access Request Form.
- All users that receive remote access will be required to take a remote access training; this training will be an annual requirement for those who need to maintain their privileged access to work remotely.

Virtual Private Network (VPN)

The remote access capabilities of all Department employees, contractors, and vendors are subject to the same security protections, policies, standards, and procedures as on-site connections. All Department information security policies, including the NYSED Acceptable Use of IT Resources policy, are applicable to the remote access environment. The following controls are required for all VPN connections:

- Remote access permissions must be associated with a single remote user and/or system.
- Remote access authorization must not be transferred to or used by another person.
- Authorized requests for non-Department employees (vendors, contractors, consultants, etc.) for VPN privileges must be requested by the business unit manager who requires the Department non-employee to have access. This request must be based on a business need. Approval by the Director of Operations (or the Deputy Commissioner), and the Information Security Office (ISO) is required. Further, an Information Protection Agreement (IPA) will need to be completed.
- VPN access requires strong authentication. See the Department User Account Password Policy for details.
- Users with remote access will receive required software and instructions for use from the desktop support team.
- Remote connections for contractors and other temporary employees using approved non-Department issued devices must be implemented using either Secure Sockets Layer (SSL) VPN portal connection or through a Citrix solution such as XenDesktop or XenApp.
- Department-issued laptops, computers, or workstations that connect remotely must have up-to-date anti-virus signatures and properly patched and updated versions of the operating systems and programs.
- VPN client connections must have an idle timeout.

Direct External Vendor Access

The following controls must be followed in situations where access to an external vendor's application requires non-Department equipment to be connected to the Department's network. For example, access to other financial institution's applications or file transfers may require direct access from the vendor's networks to the Department's network.

- The external vendor will be required to limit outbound traffic (into the NYSED network) to only the clients and services necessary to support the target application. The Department must not allow a

wide range of the vendor's Internet addresses to access the Department's network; only the required addresses will be allowed.

- All external vendor circuits and equipment will terminate on a common network segment, which will be segregated from the rest of the network by a firewall.
- Firewall rules will limit traffic to that which is required for the target application.
- Firewall rules will be applied on both incoming and outgoing network traffic to ensure security of the network and to ensure that external vendors are properly limiting access through their equipment.

Remote Support Sessions

Remote support sessions may be required for vendors or other support persons to remotely connect to a Department system to resolve a problem. A remote support session (e.g. GoToMeeting, Cisco WebEx, etc.) may include screen sharing and/or remote control. The following security controls are required when a remote session is needed:

- Any remote session requiring direct access to a Department IT resource (e.g. a personal computer (PC) or server) must be approved by the Information Security Office.
- All remote support sessions must be conducted through an SSL/TSL or other encrypted connection.
- When a vendor requires a remote support session, a session log must be enabled for the whole session.
- While a remote support session is in progress, all activity must be physically monitored by a Department employee to ensure that no inappropriate access or activities take place.
- Any window or file that is not involved in the remote support session must be closed prior to allowing remote access to the system.

4.0 Compliance

This standard shall take effect upon publication. The Information Security Office (ISO) shall review the standard at least every two years to ensure relevancy. To accomplish this assessment, the ISO may issue, from time to time, requests for information to other office departments, which will be used to develop any reporting requirements as may be requested by the Department Chief Privacy Officer, the Board of Regents, or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, the office shall request an exception through the NYSED Information Security Exception Standard process.

Any violation of this standard may subject the user to disciplinary action up to and including termination. The Department will review alleged violations of this standard on a case-by-case basis and pursue recourse, as appropriate.

5.0 Definitions of Key Terms

Information Technology (IT) Resources: Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

Virtual Private Network (VPN): A secure private network that uses the public communications infrastructure to transmit data.

6.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
Website: <http://atwork.nysed.gov/iso/>
Email: infosec@nysed.gov

7.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
8/10/2017	Draft	CISO
3/12/2019	Updated ISO Office and phone number, updated information in Section 1, and 4	Marlowe Cochran, Chief Information Security Officer
7/8/2019	Reviewed, Removed remote session timeout	ITS, CPO, CISO
11/25/2019	Updated Contact Information	Marlowe Cochran, Chief Information Security Officer
12/5/2019	Original Standard Release	Marlowe Cochran, Chief Information Security Officer
11/8/2022	Updated address and version number	Information Security Office
11/8/2024	Scheduled policy review	

8.0 Related Documents

- NYSED Information Security Standard
- NYSED Acceptable Use of Information Technology (IT) Resources Standard
- NYSED User Account Password Policy
- NYSED Information Protection Agreement Procedure