NEW YORK STATE EDUCATION DEPARTMENT'S

DATA PRIVACY AND SECURITY POLICY

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

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

1.2 OBJECTIVE

The objective of this policy is to address SED's responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its IT assets Od/T1_68e0ilamf260 1 Tf2l.5in

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 rof 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, Chief and/or e

s o n
n

3.3 PRIVACY AND SECURITY RISK M0003>]TJ 8.5olicy

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 training Effective

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 [illegible]

–

–

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 nonAð 6Á maint

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 includin5nd r 11.957_30

Hardware	The physical components of an information system. See Software and Firmware
Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security	The protection of information and information sy [tin( )T(a)]TJ EMC 0.0061 Tc 0.5870 Td

e.g.,/TT2 1 [illegible]

Information System Component	A discrete, identifte,i

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 rrepudiation	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 r to rknow, 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 a	T h The loss of confidentiality, integrity, or availability could be expectne 1 Td [(1 TdTd d o 8 e j

mother's

	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.
Sanitization	Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, the

Secguard [illegible] 0 1f (1 Tf ( )T ( )Tj /TT2 1 Tf 4.397 0 Td (to)Tj /T1_0 1 T

_0 11BDC TT2 1 Tf -requirTf 0. Tc -25.545 -1.222 Td ((Control)Tj /T1_5 1 Tf ( )Tj EMC /P <</MCID 1Tc (/T52 1 Tf 0.001 Tc -35.871 -3.7

r e s c r i b e d t h e

r [illegible]

orise T 1.2 J_0 1_01 ch.

[illegible]

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.