

Information Security Policy

New York State Education Department

(Endorsed by the Information Management Advisory Council January 3, 2002)

I – Purpose and Background

The purpose of this policy is to articulate New York State Education Department (SED) requirements for information security. The policy applies to all 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. The policy 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. The policy also provides staff with an understanding of the vulnerabilities and risks associated with information security and the appropriate steps to be taken to protect information resources.

The purpose of information security is to protect information from accidental or malicious disclosure, modification, or destruction. Information will be protected based on its sensitivity and/or confidentiality, the risk of loss or compromise, and any significant potential impact on the business of SED. Information security management enables information to be shared while ensuring protection of the information and the associated computer assets. SED Management is committed to advocating and requiring compliance with the Department Information Security Policy. The policy does not in any way interfere with the proper exercise of employees' rights under law and regulation.

Department Policy

All information, regardless of form or format, created or used in support of SED business activities, is Department information.

Department information is an asset that must be protected. Information must be maintained in a secure, accurate, and reliable manner, and be readily available for authorized use.

SED management is responsible for ensuring appropriate controls are in place to preserve the security objectives of confidentiality, integrity, and availability for SED's information assets.

All users are responsible for reading the security policy and complying with its terms.

II – Information Security Mission Statement

The New York State Education Department information security mission is to safeguard the confidentiality, integrity, and availability of Department information.

Within the scope of this mission, confidentiality, integrity, and availability are defined as:

Confidentiality – Information protected by law and is not disseminated beyond those users who are authorized to access it.

Integrity – Information retains its original level of accuracy and has not been exposed to accidental or malicious alteration or destruction.

Availability – Information will be accessible and usable on demand by authorized users.

III – Information Classification Levels

All Department information, both electronic and non-electronic, should be evaluated by the responsible Deputy and assigned a classification level. The 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, 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.

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.

IV – Responsibilities

Information and System Users

Individuals who use SED’s information and systems are responsible for adhering to all policies, standards, and procedures for securing and using information and systems, including but not limited to the following:

Users shall:

- Maintain information and system confidentiality, including security controls and passwords
- Use SED information and systems for business purposes only
- Respect the legal protection provided to systems and information by copyright and license
- Protect information from unauthorized use or disclosure as required by state and federal laws and agency regulations
- Safeguard accounts and passwords. Any user changes of a password must follow published guidelines for good passwords. ([Password Policy and Guidelines](#)) Accounts and passwords are normally assigned to single users and should not be shared with any other person
- Report any observations of attempted security violations or activities that may compromise information security
- Recognize that a workstation can be an entry point to other network devices, some of which might have confidential information, and secure the workstation as if it held confidential information
- Use access authority only for purposes related to job duties. Information is viewed and modified only as appropriately authorized

Users shall not:

- Use SED information and systems for activities unrelated to official assignments and/or job responsibilities
- Engage in illegal activities
- Transmit threatening, obscene, or harassing materials or correspondence
- Distribute private, confidential or protected information
- Interfere with or disrupt network users, services, or equipment
- Transact private business or any activity intended to foster personal gain
- Solicit for religious or political causes
- Intrude, “hack”, or knowingly install a virus on the network
- Make SED confidential information under law available to unauthorized outside parties, or load SED information on hardware components not owned by SED, without management approval

The following are examples of specific activities that are prohibited under this policy:

- Downloading unauthorized software, games, or screen-savers
- Using live streaming non-work related video or audio
- Attempting to access confidential information without proper authorization
- Intentionally altering or destroying data
- Any effort to subvert or circumvent security mechanisms
- Any illegal activities
- Running a personal business on Department equipment and time
- Downloading or viewing pornography

Information Security Officer (ISO)

The Information Security Officer is responsible for ensuring that information security policies and procedures are established and implemented to protect the information assets of the Department; participating in the creation and review of the policies and procedures; recommending security strategies; and keeping information security systems current. The Department must have procedures to prevent, detect, contain, and recover from information security breaches both from internal and external sources and disasters, both natural and man-made.

If a violation of the Information Security Policy occurs, information regarding the violation is to be provided to the ISO. The ISO will review the information and develop a plan for corrective action depending on the nature of the violation. Violations of this Policy may be referred to the Office of Human Resource Management (OHRM) for resolution.

Office of Human Resources Management (OHRM)

The Office of Human Resources Management will be responsible for any personnel issues arising from intentional or repeated violations of SED information security policies and procedures. OHRM will take appropriate administrative action, including formal discipline and/or legal action. The actions taken by OHRM may range from counseling and suspension of user access, to discipline, which can include suspension, termination or legal action for more serious violations.

Office of Audit Services

The Office of Audit Services may periodically evaluate controls and procedures and test compliance with information protection policies, standards, and procedures to appraise the adequacy of and compliance with security controls.

V – Security Awareness and Training

Security awareness and the associated responsibilities must be conveyed to all SED staff. All employees, agents, consultants, and others who access agency computer systems must

be provided with sufficient training and/or supporting reference materials to allow them to properly protect SED information.

The Information Security Officer (ISO) is responsible for a structured security awareness-training program. All SED employees will be provided with appropriate training. Employees will acknowledge participation and successfully complete the training. Security awareness training will become part of orientation for new employees.

VI – Physical Access Security

Appropriate safeguards will be implemented to limit unauthorized physical access to any Department information, computer, or computer-related device.

VII – Department Security Management and Procedures

- **Employment Changes.** Changes in employment status or job duties must include proper notification of the Information Security Officer in order to change security status.
- **Audit Trails.** The Department must maintain audit trail records sufficient to meet the requirement of the law, the needs of the Department's internal controls and audit requirements, control agency audit requirements, and, as necessary, disaster recovery requirements.
- **Logging.** All access to networked systems must be logged. When determined to be critical to the Department, the logging of transactions must be included regardless of the operating platform. These logs must be retrievable through clearly defined procedures and must be maintained for time periods prescribed for audit, legal, and recovery purposes. As new applications, platforms, mediums, or other technical changes to systems operations are made, consideration of logging requirements and availability must be made. Requirements for logging data must be clearly established as system, architectural, technical, or network designs are developed.
- **Lines of Communication.** Lines of communication and responsibility for Department security must be established, maintained, and clearly defined. The names and contact information for the responsible individuals will be available to SED staff. Alternative paths must be available in the absence of one of the individuals designated in the communications chain. The lines of communication must work in both directions for reporting of information security problems or the downward communication of problems, such as information security alerts and potential virus threats.
- **Logon Security.** Access to computer systems requires identification and authentication. Any exception to this rule requires appropriate approval.
- **Remote Access to Department Information.** Remote external access to a Department network that contains confidential information requires extended authentication procedures beyond usercode and password. Any method of providing this remote access, such as modems, requires approval prior to its installation.

- **Transaction Controls and Database Security.** Transactions entered into the Department's production databases must be checked for accuracy and authenticity. Database administrators shall implement security and authorization subsystems adequate to protect against unauthorized access and modification.
- **Downloading Software.** Only authorized individuals may download executable software from external sites.
- **Non-Department Owned IT Components.**
 - Confidential data should not be stored on non-Department hardware.
 - Non-Department software will not be installed on Department equipment.
 - Department staff, vendors, and contractors will adhere to vendor copyright and licensing agreements.
 - Non-Department hardware, such as Flash drives, external hard drives, PDAs, and other types of computer peripherals or accessories, should not be connected to Department hardware.
- **Disposal of Department IT Components.** Department hardware must be cleansed (sanitized) before being reassigned or discarded. Adequate documentation must be maintained of hardware/software taken off-site by Department employees.
- **Electronic Communications.** When transmitting confidential information on an external network, a technology must be employed to render the information unusable to an unauthorized or intercepting third party.
- **Virus Protection.** All agency computers must be equipped with up-to-date and active virus protection software.

VIII – Data Exchange Agreements

Agency Agreements. Systems that exchange data with/to any other entity must be accompanied by a signed written agreement that the entity will adhere to specific agreed upon security protocols related to the data exchange.

Third Party Agreements. All agreements with third parties such as vendors, other government agencies, or contractors must include requirements to adhere to Department information security policies or other appropriate confidential security protocols.

All vendor agreements shall contain a requirement that any Department information obtained or created as a result of such an agreement shall be the property of the Department and shall not be used, including but not limited to secondary release or disclosure, without written authorization of the Department.

Password Policy and Guidelines

New York State Education Department

POLICY

A critical part of any successful information security program is the creation and maintenance of strong passwords, both by users and system administrators. A password is used to authenticate or identify an individual. Each individual is responsible for selecting and protecting passwords that provide security for the information systems they access.

PROCEDURES AND GUIDELINES

- Passwords are not to be shared with other individuals, either inside or outside the Department.
- A password is not to be written down or posted in an individual's work area.
- Each individual is directly responsible for use of their passwords. Any action or activity taken with a password will be attributed to the owner of the password.
- A strong password conforms to the following recommended practices:
 - Contains 8 characters minimum
 - Has a combination of alpha and numeric characters; special characters, such as commas, hyphens, underscores, etc., add strength to a password
 - Uses upper and lower case letters, when available
 - Is not a proper name or any form of a individual's userID
 - Does not include a dictionary word
 - Does not substitute numbers for letters, e.g. 0 for O, 3 for E, 1 for I or L
 - Is not a previously used password.
- Passwords issued by ITS (including the Help Desk) should be changed as soon as possible.
- SED network passwords must be changed at least every 180 days; it is recommended that all other passwords (such as GroupWise) be changed at the same time.
- The Department suggests that you use a combination of letters, numbers and special characters. Avoid using single whole words. An example of a good password would be to break a word or name (even your son's or daughter's name) into two parts while adding a couple numbers and special characters (e.g. use the name "James" to create the password "ja6=7mes" or better yet "ja6[=7meS"). Another idea for creating a good password is to select a phrase that means something to you and use the first letter or each word (mixing up the upper and lower case) and then, add one or two numbers (e.g. "I love my 2009 bright red car" might be transformed into "ILM09brc") and maybe throw in a special character (e.g. "I love my 2009 bright red car" might be transformed into "ILM-09brc").

Passwords that follow these guidelines are more difficult to crack or guess, and provide a higher level of security for the Department's information assets.