NYSED Information Security Policy

(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

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 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 Resources 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 must 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.