

	POLICY # 13-01	STATUS:	ISSUED: October 2013	LAST REVISED:	PAGE: 1 of 2
	Office of Data & Analysis, Research				
RHODE ISLAND DEPARTMENT OF ELEMENTARY AND SECONDARY EDUCATION		TITLE: Data Security Policy			

1.0 Purpose

Information and information technology (IT) systems are essential assets of the Rhode Island Department of Elementary and Secondary Education (RIDE) and vital resources to Rhode Island citizens. These assets are critical to the services that agencies provide to citizens, businesses, and educational institutions, as well as to local and federal government entities. All information created with RIDE resources for State educational operations is the property of the State of Rhode Island. All employees and contractors of RIDE are responsible for protecting information from unauthorized access, modification, disclosure and destruction. This Policy sets forth minimum level of security requirements that, when implemented, will protect the confidentiality, integrity and availability of RIDE information assets.

2.0 Objectives

RIDE manages many data repositories designed to collect data, store data, provide access to data and compile and report data. RIDE data repositories include data relating to schools, students, and personnel. The RIDE Director of Data and Analysis is the designated authority to establish and maintain a system of data protections for RIDE's data repositories in accordance with the Family Educational Rights and Privacy Act (FERPA), the Rhode Island Educational Records Bill of Rights Act and other applicable state and federal laws. This Data Security Policy has been established by RIDE to ensure that all data in its repositories are securely maintained, to provide safeguards for all confidential and personally identifiable information and to ensure intended use of data.

3.0 Scope - Data Security

Security includes the technical measures put into place by RIDE to ensure that records are not lost, stolen, vandalized or illegally accessed. Since the data are stored on computers, RIDE ensures a high level of protection through secure firewalls, secure socket layers passwords, and restricted server room access. RIDE's Information Technology (IT) security system shall ensure the following elements.

- (1) Secure user authentication protocols including:
 - (a) direct access to RIDE databases, RIDE servers and RIDE stand-alone computers through active directory authentication
 - (b) requirement of a strong password to access RIDE web-based systems
 - (c) control of passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect
 - (d) managing user access to applications; and
 - (e) blocking access to users after multiple unsuccessful attempts;
- (2) Secure access control measures that:
 - (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are designed to maintain the integrity of the security of the access controls;
- (3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- (4) Monitoring of systems, for unauthorized use of or access to personal information;
- (5) For files containing personal information on a system that is connected to the Internet, up-to-date firewall protection and operating system security patches, designed to maintain the integrity of the personal information.
- (6) Up-to-date versions of system security agent software which include malware protection and up-to-date patches and virus definitions, that is set to receive the most current security updates on a regular basis.
- (7) Education and training of employees, as needed, on the proper use of the computer security system and the importance of personal information security.