I. Purpose & Applicability

A. This document defines minimum standards ("Standards") for the privacy and security of student and employee information for Local Education Agencies ("LEA") that the Department is required to establish according to New Hampshire Revised Statutes Annotated (RSA) 189:66, V.

B. These Standards apply to "Student Personally-Identifiable Data" and "Teacher Personally-Identifiable Data" (RSA 189:65), as well as "Covered Information" (RSA 189:68) handled by LEAs in both electronic and physical formats. Unless otherwise noted, the terms "Covered Information" shall include Student and Teacher Personally-Identifiable Data throughout this document.

C. All LEAs under the purview of the New Hampshire Department of Education are required to implement these Standards.

II. Minimum Privacy and Security Standards

These Standards have been developed from a subset of basic and derived security requirements from National Institute of Standards and Technology Special Publication 800-171 Revision 1, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." More information about each security standard can be found at the reference listed from NIST SP 800-171. LEAs are encouraged to review and incorporate additional security requirements from NIST SP 800-171, as appropriate.

A. Access Control

1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). (NIST SP 800-171: 3.1.1)

2. Limit system access to the types of transactions and functions that authorized users are permitted to execute. (NIST SP 800-171: 3.1.2)

3. Employ the principle of least privilege, including for specific security functions and privileged accounts. (NIST SP 800-171: 3.1.5)

4. Limit unsuccessful logon attempts. (NIST SP 800-171: 3.1.8)

5. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. (NIST SP 800-171: 3.1.13)

6. Authorize wireless access prior to allowing such connections. (NIST SP 800-171: 3.1.16)

7. Protect wireless access using authentication and encryption. (NIST SP 800-171: 3.1.17)

B. Awareness and Training

1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. (NIST SP 800-171: 3.2.1)

2. Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. (NIST SP 800-171: 3.2.2)

C. Audit and Accountability

1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. (NIST SP 800-171: 3.3.1)

2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. (NIST SP 800-171: 3.3.2)

D. Configuration Management

1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. (NIST SP 800-171: 3.4.1)

2. Establish and enforce security configuration settings for information technology products employed in organizational systems. (NIST SP 800-171: 3.4.2)

3. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. (NIST SP 800-171: 3.4.7)

E. Identification and Authentication

1. Identify system users, processes acting on behalf of users, and devices. (NIST SP 800-171: 3.5.1)

2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. (NIST SP 800-171: 3.5.2)

3. Enforce a minimum password complexity and change of characters when new passwords are created. (NIST SP 800-171: 3.5.7)

F. Incident Response

1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. (NIST SP 800-171: 3.6.1)

2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. (NIST SP 800-171: 3.6.2)

G. Maintenance

1. Perform maintenance on organizational systems. (NIST SP 800-171: 3.7.1)

2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. (NIST SP 800-171: 3.7.2)

3. Ensure equipment removed for off-site maintenance is sanitized of any Covered Information in accordance with NIST SP 800-88 Revision 1. (NIST SP 800-171: 3.7.3)

H. Media Protection

1. Protect (i.e., physically control and securely store) system media containing Covered Information, both paper and digital. (NIST SP 800-171: 3.8.1)

2. Limit access to Covered Information on system media to authorized users. (NIST SP 800-171: 3.8.2)

3. Sanitize or destroy system media containing Covered Information in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse. (NIST SP 800-171: 3.8.3)

4. Control access to media containing Covered Information and maintain accountability for media during transport outside of controlled areas. (NIST SP 800-171: 3.8.5)

I. Personnel Security

1. Screen individuals prior to authorizing access to organizational systems containing Covered Information. (NIST SP 800-171: 3.9.1)

2. Ensure that organizational systems containing Covered Information are protected during and after personnel actions such as terminations and transfers. (NIST SP 800-171: 3.9.2)

J. Physical Protection

1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. (NIST SP 800-171: 3.10.1)

2. Protect and monitor the physical facility and support infrastructure for organizational systems. (NIST SP 800-171: 3.10.2)

K. Risk Assessment

1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of Covered Information. (NIST SP 800-171: 3.11.1)

2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. (NIST SP 800-171: 3.11.2)

3. Remediate vulnerabilities in accordance with risk assessments. (NIST SP 800-171: 3.11.3)

L. Security Assessment

1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. (NIST SP 800-171: 3.12.1)

2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. (NIST SP 800-171: 3.12.2)

3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. (NIST SP 800-171: 3.12.3)

M. System and Communications Protection

1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. (NIST SP 800-171: 3.13.1)

2. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). (NIST SP 800-171: 3.13.6)

3. Protect the confidentiality of Covered Information at rest. (NIST SP 800-171: 3.13.16)

N. System and Information Integrity

1. Identify, report, and correct system flaws in a timely manner. (NIST SP 800-171: 3.14.1)

2. Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems. (NIST SP 800-171: 3.14.2)

3. Monitor system security alerts and advisories and take action in response. (NIST SP 800-171: 3.14.3)

4. Update malicious code protection mechanisms when new releases are available. (NIST SP 800-171: 3.14.4)

APPENDIX A

GLOSSARY

authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
availability	Ensuring timely and reliable access to and use of information.
confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
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 system.
external system	A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
external system service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
external system service provider	A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
external network	A network not controlled by the organization.
incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a 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 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 system	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
information technology	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 *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
internal network	A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
least privilege	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
media	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 a system.
multifactor authentication	Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric).
network	A system 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 a 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).
privileged account	A system account with authorizations of a privileged user.
privileged user	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
remote access	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
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. System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems. Such risks reflect the potential adverse impacts to organizational operations, 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 a 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.
sanitization	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
security control	A safeguard or countermeasure prescribed for a system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
security control assessment	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for a system or organization.
system component	A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building

	block of a system. System components include commercial information technology products.
user	Individual, or (system) process acting on behalf of an individual, authorized to access a system.