NEW YORK STATE EDUCATION DEPARTMENT 89 Washington Avenue, Albany, NY 12234 Telephone: (518) 474-0937 Email: privacy@nysed.gov	**DATA PRIVACY AND SECURITY POLICY**

I. Purpose

This policy addresses NYS Education Department's (the Department or SED) responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems and information technology resources.

II. Policy Statement

It is the responsibility of SED:

(1) to comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information;
(2) to maintain a comprehensive Data Privacy and Security Program designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support the Department's mission;
(3) to protect personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure;
(4) to address the adherence of its vendors with federal, state and SED requirements in its vendor agreements;
(5) to train its users to share a measure of responsibility for protecting SED's data and data systems;
(6) to identify its required data security and privacy responsibilities and goals, integrate them into relevant processes, and commit the appropriate resources towards the implementation of such goals; and
(7) to communicate its required data security and privacy responsibilities and goals and the consequences of non-compliance, to its users.

III. Standard

SED will utilize the National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

IV. Scope

The policy applies to SED employees, and also to independent contractors, interns, volunteers (" Users") and third-party contractors who receive or have access to SED's data and/or data systems.

This policy encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of the educational agency and it addresses all information, regardless of the form or format, which is created or used in support of the activities of an educational agency

This policy shall be published on the SED website and notice of its existence shall be provided to all employees and Users.

V. Compliance

Deputy Commissioners of Education are responsible for the compliance of their programs and offices with this policy, related policies, and their applicable standards, guidelines and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and program offices will be directed to adopt corrective practices, as applicable.

VI. Oversight

SED's Chief Privacy Officer shall annually report to its Board of Regents on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint submitted pursuant to Education Law §2-d.

VII. Data Privacy

(1) Laws such as the Family Educational Rights Privacy Act (FERPA), NYS Education Law §2-d and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.

(2) Data protected by law must only be used in accordance with law and regulation and SED policies to ensure it is protected from unauthorized use and/or disclosure.

(3) SED has established a Data Governance Team to manage its use of data protected by law. The Chief Privacy officer and the Data Governance Team will, together with program offices, determine whether a proposed use of personally identifiable information would benefit students and educational agencies, and to ensure that personally identifiable information is not included in public reports or other public documents, or otherwise publicly disclosed;

(4) No student data shall be shared with third parties without a written agreement that complies with state and federal laws and regulations. No student data will be provided to third parties unless it is permitted by state and federal laws and regulations. Third-party contracts must include provisions required by state and federal laws and regulation.

(5) The identity of all individuals requesting personally identifiable information, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with SED procedures.

(6) It is SED's policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, SED shall ensure that its contracts require that the confidentiality of student data or teacher or principal APPR data be maintained in accordance with federal and state law and this policy.

(7) Contracts with third parties that will receive or have access to personally identifiable information must include a Data Privacy and Security Plan that outlines how the contractor will ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.

VIII. Incident Response and Notification

The Department will respond to data privacy and security critical incidents in accordance with its **Data Breach and Cyber Incident Response Policy.** All breaches of data and/or data systems must be reported to the Chief Privacy Officer, Chief Information Officer, and Chief Information Security Officer. All breaches of personally identifiable information or sensitive/confidential data must be reported to the Chief Privacy Officer. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal PII as defined by Education law §2-d, or any SED sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.

State and federal laws require that affected individuals must be notified when there has been a breach or unauthorized disclosure of personally identifiable information. Upon receiving a report of a breach or unauthorized disclosure, the Executive Deputy Commissioner, Chief Privacy Officer, Counsel and other subject matter experts will determine whether notification of affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay.

IX. Acceptable Use Policy, Password Policy and other Related Department Policies

(1) Users must comply with the **Acceptable Use Policy** in using Department resources. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with State Entity missions and business functions (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the agency or moved to another department.
(2) Users must comply with the **Password Policy**.
(3) All remote connections must be made through managed points-of-entry in accordance with the **Remote Access Policy**.

X. Training

All users of department data, data systems and data assets must annually complete the information security and privacy training offered by the department. Information security and privacy training will be made available to all users. Employees must complete the training annually.