

Book	Policy Manual
Section	FOR BOARD APPROVAL - Volume 38, No 2, April 2026
Title	Updated Copy of INFORMATION SECURITY
Code	po8305
Status	
Adopted	April 5, 2022

8305 - INFORMATION SECURITY

The School Corporation collects, classifies, and retains data/information from and about students, staff, vendors/contractors, and other individuals, about programs and initiatives undertaken by the school system, and about and related to the business of the Corporation. This information may be in hard copy or digital format, and may be stored in the Corporation or offsite with a third party provider.

Data/Information collected by the Corporation shall be classified as Confidential, Controlled, or Published. The Superintendent shall define "Confidential," "Controlled," and "Published" in administrative guidelines and provide examples of data/information in each classification. Data/Information will be considered Controlled until identified otherwise.

Protecting Corporation data/information is of paramount importance. Information security requires everyone's active participation to keep the Corporation's data/information secure. This includes School Board members, staff members/employees, students, parents, contractors/vendors, and visitors who use Corporation Technology and Information Resources. If an employee suspects, discovers, and/or determines that a security breach has occurred, the employee shall promptly notify the employee's immediate supervisor and the Superintendent. The employee should follow up their oral notification in writing. The Superintendent will determine and implement the steps necessary to correct the unauthorized access and, as applicable, provide notification to those individuals whose personal information may have been compromised. The Corporation will work to protect the data/information, computer network or system from attack vectors, or methods by which the computer network or system is attacked, infiltrated, or otherwise compromised.

A cybersecurity incident is a malicious or suspicious occurrence that consists of one (1) or more of the categories of attack vectors and are defined as websites that:

- A. jeopardize or may potentially jeopardize the confidentiality, integrity, or availability of an information system, an operational system, or the information that such systems process, store or transmit;
- B. jeopardizes or may potentially jeopardize the health and safety of the public; or
- C. violate security policies, security procedures, or acceptable use policies (See Policy 7540.03 - Student Acceptable Use Policy/Policy 7540.04 - Staff Acceptable Use Policy).

A cybersecurity incident may consist of one (1) or more of the following categories of attack vectors: 1) ransomware; 2) business email compromise; 3) vulnerability exploitation; 4) zero-day exploitation; 5) distributed denial of service; 6) website defacement; or other sophisticated attacks as defined by the Chief Information Officer (CIO) and identified by the Corporation on its website.

~~Individuals~~ Staff members and individuals associated with the Corporation through their affiliation with a Corporation contractor/vendor who are granted access to data/information collected and retained by the Corporation must follow established procedures so that the information is protected and preserved. Board members, administrators, and all Corporation staff members, as well as contractors, vendors, and their employees, granted access to data/information retained by the Corporation are required to certify annually that they shall comply with the established information security protocols pertaining to Corporation data/information. Further, all ~~individuals~~ persons granted access ~~to~~ by the Corporation to Confidential Data/Information retained by the Corporation must certify annually that they will comply with the information security protocols pertaining to Confidential Data/Information. ~~Completing~~ For staff members ~~completing~~ the appropriate section of the Staff Technology Acceptable Use and Safety form shall provide this certification.

All Board members, staff members/employees, students, contractors/vendors, and visitors who have access to Board-owned or managed data/information must maintain the safety and security of that data/information and the Corporation Technology Resources on which it is stored. The Superintendent shall conduct an annual risk assessment related to the access and security of the Corporation's Data/Information. Further, the Corporation will maintain audit logs for access to Confidential Data/Information and regularly review such logs to detect unauthorized activity.

Corporation information security procedures shall comply with applicable Federal and State law, including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA"), Protection of Pupil Rights Amendment ("PPRA"), and Children's Online Privacy Protection Act ("COPPA").

If an individual has any questions concerning whether this policy and/or its related administrative guidelines apply to him/her or how they apply to him/her, the individual should contact the Corporation's Technology Director or Information Technology Department/Office.

The Board authorizes the Superintendent to develop administrative guidelines that set forth the internal controls necessary to provide for the collection, classification, retention, access, and security of Corporation Data/Information. Within the established administrative guidelines, the Superintendent will determine a method for maintaining a repository of cybersecurity incidents.

~~Further, the Superintendent is authorized to develop procedures that would be implemented in the event of an unauthorized release of data/information. These procedures shall comply with the Corporation's legal requirements if such a breach of personally identifiable information occurs.~~ Further, the Superintendent is charged with developing a program and/or procedures that can be implemented in the event of a cybersecurity incident, whether it involves an inadvertent or intentional unauthorized release or breach of data/information. The program/procedures shall comply with the Corporation's legal requirements as delineated below. In particular, in the event of a breach involving personally identifiable information, the Corporation shall notify affected individuals and/or government officials in accordance with State and Federal law.

Cybersecurity incident means any of the following:

- A. A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
- B. A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
- C. A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
or
- D. Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by:
 - 1. a compromise of a cloud service provider, managed service provider, or other third party data hosting provider; or
 - 2. a supply chain compromise.

Cybersecurity incident does not include mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, State, local, tribal, or territorial government entity.

Ransomware incident means a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a political subdivision's information technology systems or data and thereafter, the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

Cybersecurity Program

The Corporation's cybersecurity program shall be designed to safeguard the Corporation's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The program shall be consistent with generally accepted best practices for cybersecurity, such as the National Institute of Standards and Technology's cybersecurity framework and the Center for Internet Security's cybersecurity best practices, and may include, but is not limited to, the following:

- A. Identify and address the critical functions and cybersecurity risks facing the Corporation.

- B. Identify the potential impacts of a cybersecurity breach.
- C. Specify mechanisms to detect potential threats and cybersecurity events.
- D. Specify procedures for the Corporation to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents.
- E. Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident.
- F. Establish cybersecurity training requirements for all Board employees; the frequency, duration, and detail of which shall correspond to the duties of each employee.

Following a cybersecurity incident or ransomware incident, the Superintendent shall notify:

- A. The Executive Director of the Division of Homeland Security within the Department of Public Safety, as soon as possible, but not later than seven (7) days after the Corporation discovers the incident.
- B. The Auditor of State, as soon as possible, but not later than thirty (30) days after the Corporation discovers the incident.

Any records, documents, or reports related to the Corporation's cybersecurity program and framework, along with the reports of a cybersecurity incident or ransomware incident addressed in the preceding paragraph, are not public records. Similarly, a record identifying cybersecurity-related software, hardware, goods, and services that are being considered for procurement, have been procured, or are being used by the Corporation, including the vendor name, product name, project name, or project description, a security record.

~~The Superintendent shall require the participation of staff members in appropriate training related to the internal controls pertaining to the data/information that they collect, to which they have access, and for which they would be responsible for the security protocols.~~ All staff members and contractors with access to Controlled and/or Confidential Data/Information must complete annual training on data privacy, information security practices (e.g., internal controls applicable to the data/information that they collect and have access to and for which they are responsible for the security protocols), and breach response protocols.

Third-party contractors/vendors who require access to Corporation Confidential Data/Information will be informed of relevant Board policies that govern access to and use of Corporation Information Resources, including the duty to safeguard the confidentiality of such data/information. Additionally, all contracts with third party contractors/vendors (e.g., technology providers) who access Corporation Data/Information shall include provisions addressing data security, breach notification, data ownership, confidentiality, and destruction upon termination. Further a contract between a technology provider and the Corporation shall ensure appropriate security safeguards for education records and include both of the following:

- A. a restriction on unauthorized access by the technology provider's employees or contractors; and
- B. a requirement that the technology provider's employees or contractors may be authorized to access education records only as necessary to fulfill the official duties of the employee or contractor.

Failure to adhere to this Policy and its related administrative guidelines ("AGs") may put Corporation data/information at risk. Employees who violate this policy and/or the administrative guidelines promulgated consistent with this policy may have disciplinary consequences imposed, up to and including termination of employment, and/or referral to law enforcement. Students who violate this Policy and/or AGs will be referred to the Corporation's disciplinary system and/or law enforcement. Contractors/vendors who violate this Policy and/or AGs may face termination of their business relationships with and/or legal action by the Corporation. Parents and visitors who violate this Policy and/or AGs may be denied access to Corporation Technology Resources.

At least annually, the Superintendent shall conduct an assessment of risk related to the access to and security of the data/information retained by the Corporation, as well as the viability of the Continuity of Organizational Operations Plan developed pursuant to Policy 8300.

© Neola 2021

Legal I.C. 4-13.1-1-1.3
I.C. 4-13.1-1-1.5
I.C. 4-13.1 -2-2