Book	Policy Manual
Section	Board Prep 40.1
Title	Copy of INFORMATION SECURITY
Code	po8305
Status	
Adopted	December 13, 1993
Last Revised	December 18, 2023

8305 - **INFORMATION SECURITY**

The District 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 District. This data/information may be in hard copy or digital format and may be stored in the District or offsite with a third party provider.

Data/Information collected by the District 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 District Information & Technology Resources (as defined in Bylaw 0100) is of paramount importance. Information security requires everyone's active participation to keep the District's data/information secure. This includes Board of Education members, staff members/employees, students, parents, contractors/vendors, and visitors who use District Information & Technology Resources (as defined in Bylaw 0100). 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.

Staff members, and individuals associated with the District through their affiliation with a District contractor/vendor, ~~Individuals~~ who are granted access to data/information collected and retained by the District must follow established procedures so that the data/information is protected and preserved. Board members, administrators, and all District staff members, as well as contractors, vendors, and their employees, granted access to data/information retained by the District are required to certify annually that they shall comply with the established information security protocols pertaining to District data/information. Further, all persons granted access by the District ~~individuals granted access~~ to Confidential Data/Information retained by the District must certify annually that they will comply with the information security protocols pertaining to Confidential Data/Information. For staff members, completing ~~Completing~~ the appropriate section of the Staff Technology Acceptable Use and Safety form (Form 7540.04 F1) 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 security of that data/information and the District Information & Technology Resources on which it is stored. The Superintendent shall conduct an annual risk assessment related to the access and security of the District's Data/Information. Further, the District will maintain audit logs for access to Confidential Data/Information and regularly review such logs to detect unauthorized activity.

District 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") regarding data breaches.

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

The Superintendent shall develop administrative guidelines that set forth the internal controls necessary to provide for the collection, classification, retention, access, and security of District Data/Information.

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 District's legal requirements as delineated below. In particular, in the event of a breach involving personally identifiable information, the District shall notify affected individuals and/or government officials in accordance with State and Federal law. ~~Further, the Superintendent is charged with developing procedures that can be implemented in the event of an unauthorized release or breach of data/information. These procedures shall comply with the District's legal requirements if such a breach of personally identifiable information occurs.~~

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 District's cybersecurity program shall be designed to safeguard the District'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 District.

B. Identify the potential impacts of a cybersecurity breach.

C. Specify mechanisms to detect potential threats and cybersecurity events.

D. Specify procedures for the District 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.~~ **~~[DRAFTING NOTE: Annual cybersecurity training provided by the State, and training provided by~~** ~~_Bridgman Public School_____~~ **~~will satisfy this requirement.]~~**

x] It is the policy of the Board – if the District is experiencing a ransomware incident - not to pay or otherwise comply with a ransom demand unless the Board formally adopts a resolution to approve such a payment or compliance with the ransom demand. If that occurs, the resolution will specifically state why the payment or compliance with the ransom demand is in the District's best interest. **[END OF OPTION]**

[DRAFTING NOTE: The Board need not include this option in its policy, but action consistent with this statement is required by law.]

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 District discovers the incident.

B. The Auditor of State, as soon as possible, but not later than thirty (30) days after the District discovers the incident.

Any records, documents, or reports related to the District'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 District, including the vendor name, product name, project name, or project description, is a security record.

All staff members **(** x**)** and contractors **[END OF OPTION]** with access to Controlled and/or Confidential Data/Information must complete **(** x**)** annual **[END OF OPTION]** 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.

~~The Superintendent shall require staff members to participate in training related to the internal controls applicable to the data/information that they collect and have access to and for which they are responsible for the security protocols.~~

Third party contractors/vendors who require access to Confidential Data/Information collected and retained by the District will be informed of relevant Board policies that govern access to and use of District Information & Technology 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 District 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 District shall ensure appropriate security safeguards for education records and includes the following:

A. a restriction on unauthorized access by the technology provider's employees or contractors;

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; and

C. a stipulation that the District owns the data/information.

Failure to adhere to this Policy and its related administrative guidelines may put data/information collected and retained by the District at risk. Employees who violate this policy and/or its related administrative guidelines may be disciplined, up to and including termination of employment and/or referral to law enforcement. Students who violate this Policy and/or its related administrative guidelines will be disciplined, up to and including expulsion and/or referral to law enforcement. Contractors/vendors who violate this Policy and/or its related administrative guidelines may face termination of their business relationships with and/or legal action by the District. Parents and visitors who violate this Policy and/or its related administrative guidelines may be denied access to the District's Information & Technology Resources.

At least annually, the ~~The~~ Superintendent shall conduct ~~a~~ an ~~periodic~~ assessment of risk related to the access to and security of the data/information collected and retained by the District.

Revised 8/14/17
Revised 7/16/18
Revised 6/26/23
T.C. 12/18/23

Cross References po0100 - DEFINITIONS