Book	Policy Manual
Section	Vol. 34 No. 1 for Board Approval
Title	Revised Policy - Vol. 34, No. 1 - November 2021 - INFORMATION SECURITY
Code	po8305
Status	
Adopted	October 12, 2017

8305 - **INFORMATION SECURITY**

The Cooperative 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**~~ **its schools**, and about and related to the business of the Cooperative. This information may be in hard copy or digital format, and may be stored in the Cooperative or offsite with a third party provider.

Protecting Cooperative data/information is of paramount importance. Information security requires everyone's active participation to keep the Cooperative's data/information secure. This includes Board of Managers members, staff members/employees, students, parents, contractors/vendors, and visitors who use Cooperative Technology and Information Resources. **The Cooperative 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 Policy7540.03 - 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 (x) Chief Information Officer (CIO) ~~**_____ [insert title] and identified by the Cooperative on its website.( )**~~

Individuals who are granted access to data/information collected and retained by the Cooperative must follow established procedures so that the information is protected and preserved. Board members, administrators, and all Cooperative staff members, as well as contractors, vendors, and their employees, granted access to data/ information retained by the Cooperative are required to certify annually that they shall comply with the established information security protocols pertaining to Cooperative data/information. Further, all individuals granted access to Cooperative Confidential Data/Information retained by the Cooperative must certify annually that they will comply with the information security protocols pertaining to Confidential Data/Information. 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 Cooperative Technology Resources on which it is stored.

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 Cooperative's Technology Director or Information Technology Department/Office.

The Board authorizes the Director to develop administrative guidelines that set forth the internal controls necessary to provide for the collection, classification, retention, access, and security of Cooperative Data/Information. ~~**Further, the Director 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 Cooperative's legal requirements if such a breach of personally-identifiable information occurs.**~~ **Within the established administrative guidelines, the Director will determine a method for maintaining a repository of cybersecurity incidents.**

Further, the Director 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 Cooperative's legal requirements if such a breach of personally-identifiable information occurs.

The Director 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.

Third-party contractors/vendors who require access to Cooperative Confidential Data/Information will be informed of relevant Board policies that govern access to and use of Cooperative Information Resources, including the duty to safeguard the confidentiality of such data/information.

Failure to adhere to this Policy and its related administrative guidelines ("AGs") may put Cooperative 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 Cooperative'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 Cooperative. Parents and visitors who violate this Policy and/or AGs may be denied access to Cooperative Technology Resources.

The Director shall conduct ~~**( ) an annual**~~ **(x)** a periodic **[END OF OPTION]** assessment of risk related to the access to and security of the data/information retained by the Cooperative, as well as the viability of the Continuity of Organizational Operations Plan developed pursuant to Policy 8300.

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

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