Canon 8 Recommended Practices and Training

1) Document all security procedures including
   a. passwords;
   b. system access procedures;
   c. encryption procedures and algorithms;
   d. data exchange protocols with partners (schools, districts, state education agencies, intermediate units, application service providers, etc.);
   e. metadata (data about data) concerning technologies, methods, operations, and data elements; and
   f. other security procedures you may have.

2) Establish a thorough and robust security plan based on an extensive risk assessment, threat analysis, and countermeasure strategy for the entire organization.

3) Establish procedures that ensure adherence to security procedures for all forms of data, including digital and print records.
   a. Employ physical security measures without exception. For example, never prop open the door to the server room when it is supposed to stay locked, and install locks and other surveillance tools to prevent unauthorized entry into secure areas.
   b. Follow all security requirements related to the use of mobile data storage devices, including laptop computers, handhelds, portable disk drives (e.g., jump drives), etc.
   c. Use required transmission protocols for all forms of data exchange, including transfers of data tapes and email. This often includes the use of encryption and password privileges.
   d. Back up data responsibly. Although the organization may engage in offsite storage, individual users must be sure to store data in proper formats, in designated locations, and with appropriate testing and verification.
   e. Never allow data handlers to access data that are not required for their work.
   f. Never allow data handlers to share their passwords or other authentication information with other users who may not have the same access privileges.
   g. Never allow data handlers to use shortcuts or unauthorized channels for accessing the organization's systems and networks, whether onsite or remotely.
   h. Destroy data that have reached the end of their useful life.
   i. Review and reauthorize user access privileges at least once a year.

4) Train all data users about their data security responsibilities.
   a. Thoroughly orient new employees to security procedures, and make sure they understand their responsibilities and repercussions for failing to observe procedures.
   b. Include security training for staff and volunteers who have access to the organization's information system. This should include what to do to protect hardware and software as well as protecting information.