Data Security and Privacy

SY 2024-2025

702 KAR 1:170

Requires that the district make the board aware prior to August 31 that it has reviewed KAR and implemented best practices

Data Security Procedures in Place

-Continuously audit current access to data by various groups and adjust as needed

-Active Directory Group Policies to reflect need for access

-Secure File Transfer Protocol

-CIO must approve programs prior to purchase to check for PII use

-Preference to organizations that have signed the Student Privacy Pledge

-Separate administrative accounts

-Completed implementation of MFA on MUNIS accounts

-Completed implementation of MFA on AD accounts

-Voluntary Audit with Censys.io to identify any security vulnerabililites

Data Security Procedures in Place

Train staff (extra training for those who have access to confidential data)

-Do not share passwords

-New password length and lifespan implemented as required by state

-Computer locking when inactive for set length of time

-Constant reminders to staff about phishing emails and data security

-Cybersecurity training for staff

Maintain “open door” policy with staff to double check anything suspicious.