To: Director of Technology

From: Charles Robbins, Standards Officer, OhCR

Date: September 28, 2023

Subject: Draft Local School District Privileged Staff with Critical Data Memo

1. The following staff members have been determined to have access to critical data. These individuals are referred to as privileged account users.
   1. Superintendent
   2. Treasurer
   3. HR Director
   4. Food Service Manager
   5. Principals
   6. Guidance Counselors
   7. Technology Director
   8. Administrative Assistants
   9. School Nurse
   10. Teachers
2. Critical data such as PII, PHI, PFI or intellectual property is owned by the individual, student, parent, or others and are protected by the school district through legal agreements. Breaches of the data records by loss, leaks, or poor techniques are required to be reported to the district under policy. Federal and State law have set the number of records breached to determine the conditions for reporting.
3. Staff with access to critical data should execute more due diligence than others. Assigned computers, Access to Systems, Access to the Cloud, Secure Networks, and Secure Work Areas are defined in the following checklist.

**Assigned Computers**

* + Privileged users only retain critical data on encrypted computers.
  + Privileged users’ computers have a remote erase application.
  + Computer screens are locked when unattended.

**Access to Systems and Cloud Accounts with Critical Data**

* + 14 or more characters smart passwords with lower case, upper case, numbers, and special characters are required.
  + Only use systems and vendors that support Multi Factor Authentication.
  + No shared passwords.
  + Access to critical data is on a need-to-know basis.
  + Privilege access to data is reviewed on a regular cycle.
  + Critical data or large money transfer need to be verified internally within the organization and externally with vendors with a second means of communication.
  + Critical data not in the current school year is archived and not found on systems.
  + Transferred data that utilized Google or District email is deleted after the sharing.

**Secure Networks**

* + Only use secure networks to transfer data such as the district’s network.
  + Offsite networks such as home, travel lodging, or other remote locations require a VPN to send critical data.

**Secure Work Area**

* + Privileged users will secure Critical data when unattended.
  + Clean desk is maintained when unattended.
  + Passwords and security keys are not left unsecure in the work area.

**Management Responsibilities**

* + A breach of critical data can result in 6 to 7 figure monetary loss to the district and is currently in the list of top five risks for organizations by insurance companies.
  + Data security like safety is the responsibility of all district personnel.
  + Supervisors are responsible for verifying non privileged users are not retaining critical data.
* Supervisors are required to regularly brief data security at meetings.
* Supervisors finding unsecure critical data need to document the event with their supervisor and determine the corrective action such as training, removal of privileged status or other course of action.

1. Exceptions can be granted to critical data rules issued to privilege users by only those individuals approved by the school district. Exceptions should be documented.