Libraries, Media and Technology Services

Security of Computer Network

The use of networked technology for a school-wide student information system to maintain attendance records, discipline records, health records, grade records, and student scheduling requires vigorous security measures. The district will use defenses to protect against viruses, malware, spyware, phishing and spam. Users are prohibited from turning off or disabling district protection systems.

Physical Security Controls

The district will use physical security controls to maintain the security of the district's confidential and critical information. The information security officer (ISO) or designee will create and maintain physical security controls that protect district servers, network routers and essential network equipment from unauthorized access or theft and damage from fire, water, extreme temperature changes and power outages. The ISO or designee will create locked, physical barriers to this equipment, such as locked doors or cages.

The ISO or designee will determine who will be allowed access to essential district equipment. Those with authorized access will be provided keys or access codes to the physical barriers. The keys and access codes cannot be shared without the ISO's or designee’s permission, and the ISO or designee must be notified immediately if the keys or access codes have been compromised. The district will record who accesses essential district equipment, electronically or otherwise, using appropriate security devices, such as keys, electronic key logs, security cameras or other appropriate measures. The ISO or designee may temporarily grant access to a vendor or other person when determined necessary. The name of the person, the reason for the access and the date and time of the access will be documented, and the ISO or designee will determine whether the person needs to be accompanied by district staff before access is granted.

Physical records that include critical and confidential information will be stored in locked cabinets or in rooms with limited access. The superintendent or designee will determine who will have access to these records and will distribute keys or access codes.

Logical Security Controls

Staff members are responsible for managing their passwords, and shall be responsible for all actions and functions performed by their user ID. School personnel must comply with all District- established rules regarding passwords. These rules will dictate the number of characters in the password, the nature of the characters used in the password and the frequency of password changes. Any school employee who suspects his/her password has been compromised must report the situation to the system administrator immediately. Intentionally divulging a password will be considered serious misconduct. The consequences of password security violations will be commensurate with the seriousness of breech.

Security Logs

The ISO or designee will identify the types of security events the district will log and monitor and will ensure that the district's network management system's logging settings are appropriately used. The district's incident logs will include appropriate information so that the district can monitor significant system events. At a minimum, the district will log access to sensitive or critical system resources or information, data breaches and compromised account credentials.

Security Audit

The ISO or designee will regularly audit the district's security controls and make adjustments as necessary. All audits will be documented.