TECHNOLOGY RESOURCES

CQ
(REGULATION)

INFORMATION TECHNOLOGY

The Superintendent of Schools or designee (normally the head of the technology department) is in charge of providing the technology environment to support the District’s goals.

DATA CENTER OPERATIONS

The IT department shall ensure that data center and telecommunication closets across the district are protected by appropriate access control which segregates and restricts access from general school or District office areas. Access to the data center must be enforced using keys, electronic card readers, or similar methods where only IT or management staff have the access necessary to perform their job functions. [See CQ (EXHIBIT)]

ACCESS CONTROL

Access to information assets must be authorized, controlled, and monitored based upon job-related function and need-to-know criteria. All information assets will be protected from unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse and denial of use.

ACCOUNT MANAGEMENT

The IT department must establish a standard for creation, administration, use and removal of accounts that facilitate access to information and technology resources at CISD ensuring an appropriate level of protection for information, systems and resources. [See CQ (EXHIBIT)]

PASSWORD STRUCTURE

Employees must not employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, words in a dictionary, derivatives of user IDs, common character sequences, personal details or any predictable phrase.[See CQ(EXIBIT)]