

TECHNOLOGY RESOURCES

CQ
(EXHIBIT)

The following exhibits are used by the District:

- Exhibit A: Password structure — 4 pages
- Exhibit B: Data center operations — 4 pages
- Exhibit B.1: Data center operations — 1 page
- Exhibit C: Account Management — 3 pages

EXHIBIT A

PASSWORD STRUCTURE

Purpose

- To establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

- The scope of this policy includes all personnel who have or are responsible for an account or any form of access that supports or requires a password, on any system that resides at any CISD's facility, has access to CISD's network or stores any non-public CISD's information.

General

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

General Password Construction Guidelines

All users at CISD should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
 - Lower case characters
 - Upper case characters
 - Numbers
 - Punctuation
 - "Special" characters (e.g. @#\$%^&*()_+|~-=\`{}[]:;'<>/ etc)
- Contain at least 12 alphanumeric characters.

Weak passwords have the following characteristics:

- The password contains less than 12 characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "<Company Name>", "sanjose", "sanfran" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

(NOTE: Do not use either of these examples as passwords!)

Password Protection Standards

- Always use different passwords for CISD accounts from other non-CISD access (e.g., personal ISP account, option trading, benefits, etc.).

- Whenever possible use different passwords for various CISD access needs. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share CISD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Information Technology Department.
- Always decline the use of the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

If an account or password compromise is suspected, report the incident to the Technology Department.

Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Shall support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval wherever possible.

Use of Passwords and Passphrases for Remote Access Users

Access to the CISD's Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the Technology Department or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

EXHIBIT B

DATA CENTER OPERATIONS

Purpose

- This guideline provides support for managing physical and environmental security controls to prevent unauthorized physical access, damage, and interruption to district's information infrastructure and information flow controlled within the datacenter.

Scope

- **The IT department** shall ensure that datacenter 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 Datacenter 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.

Guideline

Data Center Physical Control

The Information Technology department should implement an access control list that includes the name and access level of each individual granted restricted or unrestricted access. A copy of the access list should be maintained both in the Information Technology office and at the safety department. A standard process should be implemented to manage changes to the access list.

Data Center Physical Controls

Telecommunication closets are limited access areas. Telecommunication equipment and data storage devices at campuses should be located in a physically controlled area. Main cross-connect and intermediate cross-connect rooms shall be restricted to authorized personnel only with door access.

Data Center Guideline:

1. The Data Center should be alarmed with a 24/7 alerting system. The district's IT Director and the district's Risk Manager or their designee should be contacted in the event that an alarm is triggered.
2. All work areas should be kept clean and free of debris. Upon completion of any work in the room, staff performing the work should ensure they have left the area as clean as it was before their work began.

TECHNOLOGY RESOURCES

CQ
(EXHIBIT)

3. All rack enclosures should be kept neat and free of optical disks, manuals or any other object not required for the proper operation of the equipment. Doors on all racks should remain closed at all times except during performed work.
4. Cables should never be looped outside of rack enclosures. Cabling between rack enclosures of adjacent racks is accepted provided a sufficient pass-through chassis is in place.
5. The District's Data Center should have processes and facilities in place to prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failures.
6. Tailgating or Piggybacking to gain entry into a restricted area is strictly prohibited. Individuals with granted access to secure areas may not allow any other person to follow unless all individuals are granted access.
7. Data Center Room Etiquette
 - No food or drink is allowed within the Data Center.
 - No hazardous materials are allowed within the Data Center.
 - Do not power any electrical or mechanical device without proper authorization.
 - All packing material should be removed from computer equipment/components in the specified staging areas before being moved into the Data Center. This includes cardboard, paper wrap, peanuts, plastic, wood and other such materials.
 - No cleaning supply is allowed within the Data Center without prior approval. This includes water.
 - Only HEPA filter vacuums may be used inside the Data Center.
 - No cutting of any material (pipes, floor tiles etc.) should be performed inside the Data Center unless special arrangements are made in advance.
 - Boxes, tapes, CDs and other material should not be stored inside the Data Center.
 - Employees authorized to access any portion of the Data Center should only access equipment for which they are specifically responsible.
 - Communicate all problems to the IT Director or designee.
 - In the event of an emergency notify IT Director or designee immediately.
 - Do not touch a Power Distribution Unit within the Data Center.
 - Do not touch air conditioning equipment.
 - Do not open communications cabinets.

Data Center Access Authorization

All requests for access to the campus Data Center need to be approved by the IT Director, superintendent or designee. Access is restricted to specific individuals with job functions related to operating equipment in the Data Center. The IT or designee must approve all changes to physical controls, including locks and alarm codes. Data Center management and access authorization procedures should

be developed and implemented to maintain baseline security for the Data Center and the protected assets.

A Campus Limited Access Area Authorization Form needs to be completed for each employee. The form will include information pertaining to the responsibilities of those with privileged access. The supervisor of the employee shall sign the authorization form.

Data Center Access Requirements

The Data Center should be equipped with at least a numeric keypad access control. Individuals prior to being granted any unrestricted or unescorted physical access will need to have a signed confidentiality agreement on file.

Unrestricted Data Center Access

Unrestricted Access is limited to district employees, and consists of unlimited, unrestricted access to all areas within the Data Center. Personnel with unrestricted physical access are allowed un-escorted access as needed to these rooms at any time; including off-hour access to otherwise closed buildings. Unrestricted physical access is normally restricted to the System and Network Administration teams within Information Technology Departments.

Access Limited to Authorized Personnel Only

Physical access to the Data Center areas should be restricted to those with operational need to enter those spaces. Staff and Administrators should not be permitted to share their keys, key cards, access token or alarm codes and should not bring any guests into the Data Center at any time without prior approval by the IT Director or designee.

Authorization for Unrestricted and Restricted Access to Data Center Areas

Visitor Access

Anyone who does not have unrestricted or restricted authorization is considered a visitor. All visitors to the Data Center will need to adhere to facility guidelines and other best practices as detailed below:

1. Visitors that require access to the Data Center spaces should provide 5 days in advance notice prior to arrival.
2. Visitors that will be performing work or maintenance on systems or infrastructure should be validated against names provided in advance by employers.
3. All visitors to Data Center Areas will be accompanied at all times by an individual with unrestricted access and need to be entered into the visitor log. All exceptions will need to have prior approval by the Information Technology Director or designee.

TECHNOLOGY RESOURCES

CQ
(EXHIBIT)

4. Visitors will need to be signed in when entering the campus Data Center to document the time and purpose of their visit, and will need to sign out when leaving.
5. Information Technology should deny access to the Data Center to anyone who intends to install or remove equipment without some type of change management, installation form or file process being followed. Installation of unauthorized equipment without prior change management submission in the unrestricted zone during off-hours may result in a cancellation of authorization for access and removal of all unapproved equipment from the Data Center.
6. All tests required to comply with safety authorities affecting the availability of the Data Center shall be documented, communicated and approved following a change management process where the Information Technology Director is notified with twenty days advance notice.

Audit Procedures

The Information Technology Director and the District's Auditor should review the list of authorized employees twice a year and verify against signed Authorization forms.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the Technology Department or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.


	DATA CENTER ACCESS AUTHORIZATION LOG	DATE
The following individual(s) have approval for access to the CISD Data Center and have been provided a copy of the Data Center Access Policy		
Full Name	Signature	Temp ID #
1.		
2.		
3.		
Access is given for the following reason(s):		
Access is ongoing <input type="checkbox"/>	Access is time/date specific <input type="checkbox"/> Time and Date(s):	
Approved By:		
	Technology Director	
Or Approved By:		
	Administrative Services	

EXHIBIT C

ACCOUNT MANAGEMENT

Purpose

- The purpose of this guideline is to 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.

Scope

- The scope of this policy is applicable to individuals that, through the use of an account, access information and technology resources at CISD. It does not cover the authentication method used to ensure the identity of the user.

Definition

- User Account – Any combination of User ID (username) and a password that grants an individual user access to a computer, an application, the network or any other information technology resource.

General

Access Controls

- Access to the network, information systems and servers will be achieved by the use of individual user accounts that will require an appropriate authentication method as outlined in the User Password Management Policy;
- All accounts must have a password expiration that complies with CISD's User Password Management Policy
- All users must sign CISD's Acceptable Use Policy before access is given to an account
- Access to information systems will be governed by a formally defined authorization process covering the creation, modification/maintenance, re-enabling and deletion of accounts;
- Procedures will be implemented to ensure that access to data or information is not dependent on any one individual;

TECHNOLOGY RESOURCES

CQ
(EXHIBIT)

- Each assigned account will uniquely identify the user and must conform to the naming standard (first initial name/surname)
- All employees have a legal duty to keep all personal data confidential and to comply with the data protections provisions contained within CISD's Acceptable User Policy

Procedure

New Accounts

- New Employees/Employee Transfers
 - SchoolDude ticket is submitted to IT upon completion of hire/transfer for account creation including necessary information:
 - Name
 - Organization
 - Employee ID
 - Start Date
 - Upon completion of SchoolDude work order, new account information is forwarded to HR for appropriate delivery to new hire.
- Substitutes
 - New hires/hired as permanent employee:
 - SchoolDude ticket is submitted to IT upon completion of hire for account creation including necessary information:
 - Name
 - Employee ID
 - Start Date
 - Upon completion of SchoolDude work order, new account information is forwarded to HR for appropriate delivery to new hire.
- Turnaround Time
 - Minimum of 5 day notice from employee start date – hire date
 - Less than 5 day notice from employee start date – two business days after hire date

Disabling Accounts: Separations

- Upon separation processed by HR:
 - SchoolDude is submitted to IT to disable account including necessary information
 - Name
 - Organization

TECHNOLOGY RESOURCES

CQ
(EXHIBIT)

- Separation Date
 - Upon completion of SchoolDude work order, disabled account information is forwarded to HR for appropriate distribution
- Turnaround time
 - Account to be disabled upon separation date
 - Short notice separations will be addressed on a case by case basis

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. All users of CISD's information technology accounts are required to comply with this policy. CISD reserves the right to deny, to limit, to restrict or extend privileges and access to its Information Technology Accounts.