Responsible: Office of Information Technology

PURPOSE

This administrative procedure establishes the guidelines related to computer passwords in the Washoe County School District ("District" or "WCSD").

PROCEDURE

1. Passwords are an important aspect of computer security and are the front line of protection for user accounts.
2. A poorly chosen password may result in the compromise of the District's entire network. As such, all District employees, volunteers, and students (including contractors and vendors) with access to District systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.
3. The purpose of this procedure is to establish a standard for the following password settings:
    a. Minimum password length
    b. Password History
    c. Minimum password age
    d. Maximum password age
    e. Password complexity requirements
    f. Password reversible encryption
4. This procedure applies to all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides or connects to any District facility or stores any nonpublic District information.
5. Following are the recommended periods for users to change their passwords.
    a. Application Administrator Accounts passwords should change every 90 days. An application administrator account is a system account that is used solely for administration purposes of an application (e.g. BusinessPlus, MS SQL, Infinite Campus).
    b. All System level passwords privileges should change every 90 days. System level privileges allow the user to perform administration functions.

c. All Service level accounts passwords should change every 90 days. Service level accounts are used by applications development to connect to data sources.

d. All Information Technology Staff accounts shall have Multi-Factor Authentication (MFA) enabled and implemented. MFA is a 2nd means of authentication (e.g. code sent a cell phone) used in conjunction with a username and password.

e. All other Staff Accounts shall change their passwords every 90 days unless Multi-Factor Authentication (MFA) has been enabled for that account.

f. All Student Accounts shall change their passwords the week following the Fall break (on or about October) and the week following Spring break (on or about March)

6. General

a. Passwords should NEVER be written down or provided to anyone. It is recommended that administrators not require staff and students to write down their passwords at any time.

b. Passwords should NEVER be used in email messages or other forms of electronic communications.

c. The minimum password length for District staff accounts will be 8 characters.

d. Password history will be set to the maximum of 25. The system will "remember" the last 24 passwords used, not allowing any repeat of those passwords.

e. The minimum password age will be set to 30 days. As a result, passwords cannot be changed, by the user, within that 30-day period.

f. The maximum password age will be set to 90 days. Users will be reminded a week in advance to change the password.

g. Password complexity requirements will be set to Yes. Password complexity requires that upper and lower case letters, numbers, and special characters are used in a password.

h. Password reversible encryption will be set to Yes.

i. All passwords should conform to the guidelines described below

7. Guidelines for strong passwords
    a. Passwords must have a minimum of 8 characters.
    b. Characters should be a mix of upper and lower case letters (e.g., a-z, A-Z), digits and special characters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
    c. Passwords should not contain any of the following:
        i. Words found in a dictionary, of any language;
        ii. Names of family, pets, friends, co-workers, fantasy characters, etc.;
        iii. Computer terms and names, commands, sites, companies, hardware, or software;
        iv. The words "WCSD", "sanjose", "sanfran" or any derivation;
        v. Birthdays or other personal information such as addresses and phone numbers;
        vi. Word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321;
        vii. Any of the above spelled backwards; or
        viii. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
8. Password Protection Standards
    a. Do not use the same password for District accounts as for other non-District accounts (e.g. personal email, online banking, web based e-mail)
    b. All passwords are to be treated as sensitive, confidential District information.
    c. Do not do any of the following:
        i. reveal a password in an email message;
        ii. talk about a password in front of others;
        iii. hint at the format of a password (e.g., "my family name");
        iv. reveal a password on questionnaires or security forms;
        v. share a password with family members;

vi. reveal a password to co-workers while on vacation; or

vii. write down your password on a sticky note and place it under your keyboard or on your monitor to remember it.

d. If someone demands your password refer them to this document or have them call the IT Customer Help Desk at 789-3456.

e. Do not use the "Remember Password" feature of applications (e.g., Internet Explorer, Chrome, Firefox, etc.).

f. Do not store passwords in a file on ANY computer system (including phones and tablets) without encryption.

g. If your password is inadvertently revealed, change your password IMMEDIATELY.

h. If an account or password is suspected to have been compromised, report the incident to the IT Customer Help Desk at 789-3456 and change all passwords.

9. Enforcement

a. Any employee or student, found to have violated this procedure may be subject to disciplinary action as provided for in other agreements.

10. Exceptions for Testing and Kindergarten

a. New accounts have been created for elementary, middle, and high schools. These accounts will be used for testing only and will be managed by the Department of Assessment. A school that used a generic login for other purposes will now direct students to login as themselves.

i. Account Names

- testing.es
- testing.ms
- testing.hs

ii. Password – Managed by Assessment

b. An account was created to assist with Kindergarten and Pre-K students. This will allow teachers in these grade levels to train students how to login as themselves. This account will stay active for the first semester of school while students get used to the process. At the end of the semester it will be disabled automatically and students will need to login as themselves using their own username and password.

i. Account Name

- abc123

ii. Password - See your ETS

c. The use of generic accounts to access District resources is a serious security risk allowing hackers easier access to District resources. While students may not have access to sensitive information, student accounts, once compromised, can be used to escalate privileges and gain access to sensitive data.

11. NEVER share your password with ANYONE. Avoid writing your password down anywhere.

12. If you have any questions on password security contact security@washoeschools.net.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This Administrative Procedure reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District, to include:

   a. Board Policy 7205, Information Technology – Data Access

   b. Administrative Regulation 7211, Responsible Use and Internet Safety

REVIEW AND REPORTING

1. This procedure and any accompanying documents will be reviewed bi-annually in even numbered years.

REVISION HISTORY

Date	Revision	Modification
12/21/2017	v1	Adopted