Emery County School District

Policy: EHA- Employee Passwords

Date Adopted: 9 August 2017

Current Review / Revision: 10 April 2024

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of the entire Emery School District (ESD) network. As such, all ESD employees (including contractors or vendors with access to ESD systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

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 ESD facility, or has access to the ESD network.

General

- All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed frequently and cannot reuse the last 5 passwords.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed frequently and cannot reuse the past 5 passwords.
- Passwords or usernames shall not be inserted into emails or other forms of e-communication.
- All passwords must conform to the guidelines described below.

  Guidelines for Password Construction Requirements
- Be a minimum length of twelve (12) characters on all systems
- Not be the same as the User ID
- Change frequently

- Encouraged to use an encrypted password manager
- Not be transmitted in the clear or plaintext outside the secure location
- Not be displayed when entered
- Ensure passwords are only reset for authorized user

Password Deletion

All passwords that are no longer needed must immediately be deleted, disabled, or approved for other arrangements. This includes, but is not limited to, the following:

- User retirement, resignation, dismissal
- Default passwords
- Contractor accounts when no longer needed to perform their duties

  When a password is no longer needed, the following procedures should be followed:
- Employee should notify his or her immediate supervisor
- Contractor should inform his or her point-of-contact (POC)
  ESD Tech Department will then delete the user's password and delete or suspend the user's account.

Password Protection Standards

Do not use your User ID as your password. Do not share ESD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential ESD information. Here is a list of "do not's":

- Don't reveal a password over the phone to anyone
- Don't reveal a password in an email message with username
- Don't reveal a password to anyone including family, boss, co-workers
- Don' talk about a password in front of others
- Don't reveal a password on questionnaires or security forms
- Don't use the "Remember Password" feature of applications
- Don't write passwords down and store them anywhere in your office
- Don't store passwords in a file on ANY computer system unencrypted
- Don't use any password other that your own
- Use dual factor authentication when possible
- If someone demands a password, refer them to this document or have them call the ESD technology supervisor. If an account or password is suspected to have been compromised, report the incident to ESD Tech Department and change all passwords.

Application Development Standards

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

- Support of authentication of individual users, not groups

- Should not store passwords in clear text or in any easily reversible form
- Have a way to require dual factor authentication

Remote Access Users

Access to the Emery School District networks via remote access is to be controlled by using a Virtual Private Network (in which a password and user Id are required with a secondary verification before access is granted).

Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.