Instruction

Exhibit - Password

Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password and a password that does not expire may result in the compromise of Moline-Coal Valley School District's (District hereafter) entire network. It could also lead to the compromise of staff's personal, financial and professional data. As such, all adult District computer users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. All adult users will be required to change their password at designated times during the school year (TBD).

Scope

This procedure applies to all adult employees of the Moline-Coal Valley School District who have any form of computer or application account that requires password access. Examples of accounts include, but are not limited to:

- Employee workstation (desktop, laptop, tablet, Macintosh or Windows)
- Network account login
- Email
- Centralized applications (Google, Employee Portal, Student Information System)

Password Policy

General Password Guidelines

1. Passwords should not be based on well-known or easily accessible information, including personal information.
2. Moline-Coal Valley School District's centralized directory will be used to ensure that passwords meet complexity requirements as outlined below.
3. Passwords should never be shared with any other individual or group under any circumstance. Voluntarily giving password information is a direct violation of the AUP, and disciplinary action may be taken.
4. Passwords should never be written down or displayed in plain view.
5. Passwords should never be re-used. The district's centralized directory will ensure that passwords remain unique.

Moline-Coal Valley School District Password Complexity Requirements

1. Passwords are at least 8 characters long and no longer than 12 characters.
2. Passwords contain at least one upper case letter.
3. Passwords contain at least 4 numbers.

4. Passwords may not be re-used.
5. Example 1: Abcd2345

Password Protection Guidelines

1. Passwords are to be treated as confidential at all times. Under no circumstances is an employee to provide password information to another person. This includes never providing passwords to EdTech staff, Administrators, substitute teachers, student teachers, students, friends, or family. Doing so directly compromises confidential data, financial information and electronic communication.
2. Under no circumstances will any member of the Moline-Coal Valley School District (including EdTech) request a password in any electronic form. Passwords should never be shared via email, forms, or over the phone.
3. EdTech may request an employee password for troubleshooting only and only in person. Once the issue is resolved, EdTech will reset the user's password and force it to be changed again.
4. Do not use the "Remember Password" feature within online applications.
5. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the EdTech Department immediately. EdTech will reset the password and force a new password at the next login.
6. If EdTech successfully guesses or cracks a password as part of its security audits, the user will be required to change the password regardless of the password age.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action.

CABINET REVIEWED: September 2020, September 2022