PASSWORDS 1604

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees of Union Public Schools are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.

SCOPE

This policy applies to all employees of the district who have or are responsible for a computer account or any form of access that supports or requires a password on any system that resides at any district facility, has access to the Union Public Schools network or stores any non-public district information.

GENERAL

A. A password must not repeat within the last six passwords.

B. Password must not match any pattern of the previous password.

C. Passwords must contain at least fifteen (15) characters.

D. Passwords must contain at least one (1) uppercase letter (e.g., N)

E. One (1) lowercase letter (e.g., t).

F. Passwords must contain at least one (1) numerical character (e.g., 5).

G. Passwords must be at least 1 day old prior to changing password without involvement from the Technology department.

User accounts configured with mail access must change password at least once every 365 days.

PASSWORD CONSTRUCTION GUIDELINES

A. For security purposes, it is strongly recommended that passwords not be based on well-known or easily accessible personal information or that of the user's friends, family members or pets. Personal information includes, but is not limited to, log on I.D., name, birthday, address, phone number or social security number.

PASSWORD PROTECTION GUIDELINES

A. Passwords must be treated as confidential information. No employee is to give, tell or hint at their password to another person, including IT staff, administrators, superiors, secretaries, assistants, other co-workers, friends or family members under any circumstances.

B. If someone demands your password, refer them to this policy or to the IT Department.

C. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail.

D. No employee is to keep an unsecured written record of passwords, either on paper or in an electronic file.

E. Passwords used to gain access to district systems should not be used as passwords to access non-district accounts or information.

F. The password used for Union Public Schools access must be unique and not shared with any other system, website, cloud service, or app.

G. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately.

H. The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change the password immediately.

I. Only an employee's supervisor, building secretary, or other administrator can request that an employee's password be reset.

J. Passwords shall never be written on a whiteboard, interactive flat panel, chalkboard, or any other means.

MOBILE DEVICE PIN/PASSWORD CONFIGURATION STANDARDS

A. When using a mobile device, such as a smart phone or tablet, to access, manipulate, or generate district-owned data that contains any personally identifiable information, the device must require authentication prior to accessing the mobile device.

B. PINS/Passwords must be a minimum of 6 characters, employ facial recognition authentication, fingerprint reader, or complex pattern unlock feature.

ENFORCEMENT

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

Adopted 1/16/06
Revised 1/18/10
Revised 12/12/11
Revised 12/11/17
Revised 12/10/18
Revised 12/14/20
Revised 12/12/22
Revised 12/11/23