Wilson School District #7

Digital User Account Protection Policy

Date: April 02, 2021
Version: 01.2021

Overview

User Account Protection Policies are an important component of information and network security. The use of a User ID/Login and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being accessed appropriately. As such, passwords must be constructed, used, and protected appropriately to ensure that the level of security they imply is met.

Purpose and Scope

The purpose of this policy is to provide the guidelines necessary for all students, staff, and contractors of Wilson School District #7 to create, manage and protect their Digital Accounts.

This policy applies to all students, staff, and contractors of Wilson School District #7 who have any form of computer or application account that requires password access. Examples of accounts include:

- Workstation (desktop/laptop/tablet)
- E-mail system (Office365)
- Accounting application (Infinite Visions, QuickBooks, etc.)
- School Data applications (Infinite Campus)

Please note: This list is not intended to be all-inclusive; it is simply provided for reference purposes.

Policy Provisions

1. Password construction, lifecycle and re-use parameters will be variable according to the classification of the system, user, or data that they are intended to protect.
2. Passwords should not be based on well-known or easily accessible information, including personal information, nor should they be words commonly found within a standard dictionary.
3. Wilson School District #7 will use technical measures to ensure that users conform to the policy.
4. All passwords must conform to the guidelines outlined in this policy.

Account Creation Guidelines

Technology Department

Passwords used by Technology Department Staff to access Technology systems (Servers, Routers, Firewalls, Switches and Cloud Apps) must be a minimum of ten (10) characters in length. Further, these passwords must use at least three of the four-character types, those being lower case letters, upper case letters, numbers, and special characters.
All accounts should be protected by MFP (Multi Factor Authentication) if available.

Administration (Directors, Principals, Secretaries, Assistants, etc.)

Passwords used by Administration to access Workstations and all Applications must be a minimum of ten (10) characters in length. Further these passwords must use at least three of the four-character types, those being lower case letters, upper case letters, numbers, and special characters.
All accounts should be protected by MFP (Multi Factor Authentication) if available.

Basic User (Teachers, Food Service, Maintenance, IAs, Substitutes, etc.)

Passwords used by Basic Users to access Workstations and all Applications must be a minimum of ten (10) characters in length. Further these passwords must use at least three of the four-character types, those being lower case letters, upper case letters, numbers, and special characters.

Student

Passwords used by Students to access Workstations and all Applications will be set by Administration and distributed as needed.

Password Lifecycle Guidelines

Technology Department

Devices, Websites and Applications used by the Technology Department must be at minimum reset every ninety (90) days.

Administration (Directors, Principals, Secretaries, Assistants, etc.)

Devices, Websites and Applications used by Administrators must be at minimum reset every year.

Basic User (Teachers, Food Service, Maintenance, IAs, Substitutes, etc.

Devices, Websites and Applications used by Basic Users must be at minimum reset every year.

Student

Devices, Websites and Applications used by Students must be at minimum reset every year.

Password Reuse Guidelines

All passwords may be reused every third password. As such a completely new password is required for the first two expiries; thereafter the first password can be reused. “Completely new” is defined as having at least fifty percent (50%) of the characters different from the previous password.

Password Protection Guidelines

1. Passwords are to be treated as confidential information. Under no circumstances is an employee or student to give, tell, or hint at their password to another person, including IT staff, Administrators, supervisors, other co-workers, friends, and family members, except when student passwords are being distributed by their teachers or Administrators.
2. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company's Virtual Private Network or SSL-protected Web site.
3. No employee or student is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file, unless it is being protected by a district provided Secure Vault.
4. Do not use the "Remember Password" feature of applications.
5. Passwords used to gain access to company systems are not to be used as passwords to access non-company accounts or information. Similarly, passwords used to access personal, non-work-related accounts are not to be used to access company accounts.
6. Each application, system and data point should be protected by a different password where possible. The use of the same password to protect all access is strongly discouraged.
7. If an employee or student either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately.
8. The IT Department may attempt to crack or guess the passwords of Technology Department, Administration or Basic Users 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 his or her password immediately.

Enforcement

Any employee or student who is found to have violated this policy may be subject to disciplinary action. Wilson School District #7 may occasionally test users against this policy by either asking for a user's password or via a planned password phishing test.

User Agreement

As a user of Wilson School District #7's digital user accounts I understand and agree to the terms listed herein and I will follow the guidance set forth by Wilson School District #7 as it pertains to my accounts including, e-mail.

User Classification

☐ Technology Department ☐ Administration ☐ Basic User ☐ Student

Name

X _____

Signature: Date:

X _____

Review

This policy shall be reviewed annually by the Technology Supervisor and Director of Business Services and Technology and approved by the Wilson School District #7 Governing Board.

Approvals

Board Approved:
Effective Date:

Superintendent

Director of Business Services and Technology

Technology Supervisor