Wilson School District No. 7

2019 Digital User Account Protection Policy

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 actually met.

Purpose

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

Scope

This policy applies to all employees and students of Wilson School District 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

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 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 Dept.

Passwords used by Technology Dept. 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 one 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 one 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 one 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 Administrations and distributed as needed.

Password Lifecycle Guidelines

Technology Dept.

Devices, Websites and Applications used by the Technology Dept. 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 one (1) years.

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

Devices, Websites and Applications used by Basic Users. must be at minimum reset every one (1) years.

Student

Devices, Websites and Applications used Students may be at minimum reset every one hundred eighty (180) days.

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, superiors, other co-workers, friends, and family members. Except when Student Passwords are being distributed by their Teachers or Administrators

2. Under no circumstances will any member of the organization request a password in person without using the secure Password Reset Website provided by the district.

3. 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.

4. 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's being protected by a district provided Secure Vault. .

5. Do not use the "Remember Password" feature of applications.

6. 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.

7. 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.

8. 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.

9. The IT Department may attempt to crack or guess the passwords of Technology Dept. 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.

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.

Enforcement

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

Password Policy User Agreement

I hereby agree to the terms and conditions of Wilson School District 7's Password Policy.

User Classification:

Technology Dept. **Administration** **Basic User** **Student**

Employee / Student Name (print)

Employee / Student Signature

/ /

Date