مـــدرســـة الـشـــارقـــة الأمريـكـيـة الـدولـيـة
Sharjah American International School

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

Password Protection Policy - Staff

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to SAIS systems, are responsible for taking the appropriate steps, as outlinedbelow, to select and secure their passwords.

2. Purpose

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

3. Scope

The scope of this policy includes all SAIS users 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 SAISfacility, has access to the SAIS network, or stores any non-public SAIS information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

4.1.2 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.

4.1.3 User accounts that have system-level privileges granted through group memberships musthave a unique password from all other accounts held by that user to access system-levelprivileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

4.2 Password Change

4.2.1 Passwords should be changed every 90 days.

4.2.2 Passwords may not be written down, unless stored in an encrypted format.

4.3 Password Protection

4.3.1 Passwords should be treated as confidential information. No employee is to give, tell, or hint at their password to another person, including Technology staff, administrators, supervisors, other co-workers, friends, and family members, under any circumstances. If someone asks for your password, refer them to this procedure or have them contact the IT Department.

4.3.2. Passwords are not to be transmitted electronically over the unprotected Internet, such asvia e-mail.

4.3.3. No user is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept ina controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

4.3.4 Staff should not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 If an employee either knows or suspects that his/her password has been compromised, it must be reported to the Online Safety Group (by email or on Teams) and the password changed immediately.

4.3.6 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 theseaudits, the user will be required to change his or her password immediately

5. Password Reset Procedure

5.1 Staff should contact Mr. Kumar, the IT technician or Mr. Yousef, the Online Safety Officer. The request will be followed up with a return call (if the user is not their physically) to validate the user requesting the change. Upon validation, the password willbe set to a new unique password and read over the phone to the user while they are logging in. Passwords are not to be sent via email. Staff will be asked to change the password immediately after the reset is done successfully.

6. Policy Compliance

6.1 Compliance Measurement

The IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, internal and external audits, and feedback tothe principal.

6.2 Exceptions

Any exception to the policy must be approved by the IT Department in advance.

6.3 Non-Compliance

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

1st Occurrence: Verbal warning / Written Warning depending on the violation degree.
2nd Occurrence: Final Written warning, the staff member signs an undertaking.
3rd Occurrence: Dismissal from SAIS

7. Password Construction Guidelines

Passwords are used to access the network, Teams, e-mail, the Web, and voicemail.

Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

1. Passwords must contain at least 8 characters.

3. Passwords must be at least 8 characters in length and contain characters from three of the four following categories: Sample: We1come! (Do not use this sample)

a. English uppercase characters (A through Z)

b. English lowercase characters (a through z)

c. Base 10 digits (0 through 9)

d. Non-alphabetic characters (for example, !, $, #, %)

4. Passwords may not contain your First, Middle or Last name

5. Passwords should not be based on well-known or easily accessible personal information suchas date of birth or phone number.

6. Passwords should not be words that can be found in a standard dictionary (English or foreign)or are publicly known slang or jargon.

Password Creation Tips:

1. Think of a sentence that you can remember. This will be the basis of your strong password orpass phrase. Use a memorable sentence, such as "My son Aiden is three years old."

2. Check if the computer or online system supports the pass phrase directly. If you can use a passphrase (with spaces between characters) on your computer or online system, do so.

3. If the computer or online system does not support pass phrases, convert it to a password. Takethe first letter of each word of the sentence that you've created to create a new, nonsensical word.Using the example above, you'd get: "msaityo".

4. Add complexity by mixing uppercase and lowercase letters and numbers. It is valuable to usesome letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden's name, or substituting the word "three" for the Procedure: 6800.6P Page 4 of4 number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your pass phrase might become "My SoN Ayd3N is 3 yeeRs old." If the computer or online system will not support a pass phrase, use the same technique onthe shorter password. This might yield a password like "MsAy3yo".

5. Finally, substitute some special characters. You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i$ 3 yeeR$ old" or a password (using the first letter of each word)

I have read, understood, and will abide by the above Policy. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may betaken, and/or appropriate legal action may be initiated.

This policy was reviewed in August 2021.