PASSWORD PROTECTION POLICY

Passwords are an important aspect of computer security. In Scholars Indian Private School, they are the frontline of protection for user accounts.

Aim

The aim of this policy is to establish a standard for the creation of strong password, protection of these passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account on any system that resides at Scholars Indian Private School or school network.

Policy

1. The two steps verification process, ***Multi-factor authentication (OTP system)*** for all users in the Microsoft 365 learning platform is configured.
2. The ***self-service password reset*** for all users in the school website and Microsoft 365 learning platform to ensure that users are able to recover/reset their passwords themselves is enabled.
3. All system level passwords must be changed on quarterly basis.
4. All user level passwords must be changed at least every three months.
5. Each password must be unique.
6. Re-use of same password will not be allowed.
7. Passwords must be a minimum of 8 characters long.
8. Passwords should never be written down or stored online.
9. User login credentials to all students and staff to access the school online platform (Microsoft 365) with an initial temporary password which has to be changed during their first login is provided.
10. A custom alert policy in school online platform (Microsoft 365) for reviewing or resetting their Microsoft account password and email which is linked with their personal email id in every 3 months is configured.

General Password Construction Guidelines.

1. Password should not be a word in dictionary.
2. Password should not be common usage word.
3. Include uppercase and lowercase alphabets, digits and special characters.
4. Password should not be based on personal information, names of family, etc.
5. Create passwords that can be easily remembered.

Password Protection Standards

1. Do not use the same password for school accounts as for other non-school access.
2. Do not reveal a password over phone or in an e-mail message.
3. Don’t talk about it in front of others.
4. Don’t hint at the format of a password.
5. Don’t write password in a place accessible to others.

Use of Password and Passphrases

Passphrases which is a longer version of password ensure more secure data access.
All rules of passwords apply to passphrases.

Responsibilities

The IT coordinator will be responsible for the day to day management of the password security policy.
All users will have responsibility for the security of their username and password.
They:
1. Must not allow other users to access the systems using their log on details.
2. Must immediately report any suspicion or evidence that there has been a breach of security.
3. Must change their password if they are aware that it has been known by another user.

Passwords for new users and deletion of passwords no longer in use will be done by the IT Governor.

Enforcement

Any employee who violates this policy is subjected to disciplinary action and loss of network privileges.

Adopted: April, 2020 **Reviewed and updated: April, 2023**

Hameed Ali Yahya K. M.
Principal