Standard for Passphrase and Password

Parent Policy:	*Use of Information Technology Resources*		
Standard Sponsor:	College Information Officer		
Standard Contact:	Manager, IT Security		
Stakeholders:	Okanagan College Users		
Approved by:	College Information Officer		
Effective Date:	29-April-2024		
Last reviewed:	29-April-2024	Scheduled review date:	29-April-2025

1. Purpose

1.1 This defines the standards for the creation and use of passphrases to protect College electronic information that employees handle

1.2 Passphrases (sequences of words or other text) and passwords (words or strings of characters) are common and important ways to access and protect digital information on or off the internet through almost any type of device. Consequently, attackers attempting to access information use a variety of tools to guess or steal passphrases/passwords.

1.3 In summary, the top three ways to keep a passphrase/password safe and protect the information are:

a) create a strong passphrase/password

b) guard it carefully (e.g., do not share it or write it down); and

c) avoid reusing it for other systems.

2. Creating a Passphrase

2.1 Use a passphrase with a minimum of 8 characters and including a mix of uppercase, lowercase, a number and a symbol. If a minimum of 8 characters is not technically allowed by a system, use a complex password that contains upper- and lower-case letters, numbers and symbols that is as long as possible. Guidelines for consideration:

a) To create a passphrase, consider using a phrase of disconnected words that you can picture in your head (e.g., "plug-in sunshine 2 thimbles" or "4StingersSingPaint!").

b) To create a complex password when a passphrase is not an available option, consider using the first letter of each word in a phrase. For example, "I ride my bike to school at 7 AM!" becomes "Irmbtsa7AM!".

c) Avoid using a password that replaces a letter with a number, such as "Br0adcast!" where the "O" is replaced with a zero. Password guessing programs can easily crack these types of alpha/numeric replacements.

d) generation and storage programs should be used to create and manage passphrases/passwords.

e) Name, username, address, date of birth, family members' names or any other term that can be easily guessed should not be used to create a passphrase/password.

Bad Examples (Easy to Guess)	Good Passphrase Examples (Preferred)	Good Complex Password Examples
Pa$5w0rd!	pass 2 turtle phrase@	Hx%2Pe2fWE
WhiteCaps2018	trophy.sky.sings.4gold	5vE@Pu57^j
12345678ABC	1plusfourbeaches.	9#fAaXu7y6tt
GameofThrones	Facelessdragonhorse1!	p39&k1WX3EGxKo
Vanc0uv3r	Rainbeachpuddles_0	gqEWep8#32v2xF8i
2March1976	Singing1Lionor1Lamb)	Yy6*&u22rB
qwerty1234	3Elephantskickscat^	Jb06MTKS35
M0nk3yABC	MonkeyPats.Tiger1	854Htt8EvR
lLoveYou	99Mammamialetmego,	4Qz7cSPgdAB15wLm

3. Changing a passphrase/password

3.1 Passphrases/passwords on accounts protected by multi-factor authentication do not expire. For all other accounts, it is recommended that passphrases/passwords be changed annually. When changing a passphrase/password:

a) do not use a previous passphrase/password;

b) do not use the same passphrase/password for personal accounts and college accounts; and

c) it is recommended to use unique passphrases/passwords for different accounts, so that even if one is stolen, it does not allow access to other accounts owned by the same User.

d) each time a passphrase/password change or reset occurs, a multi-factor authentication (MFA) challenge is required for employee college login accounts. For all other accounts, it is recommended.

4. Protecting a passphrase/password

4.1 If a passphrase/password is written down, it must be locked away in a secure, inaccessible location such as a safe.

4.2 Best practices state that passwords should not be shared for any reason—even with trusted individuals such as supervisors or College IT Staff.

4.3 College IT Staff will never ask for Users' passphrases/passwords.

4.4 Do not respond to emails or phone calls requesting passphrases/passwords and multi-factor authentication (MFA) passcodes, even if they appear to be from a trusted source. These requests are often attempts to steal Users' credentials.

4.5 Passphrases/passwords must be immediately changed if there are suspicions that they could have been compromised and the incident must be reported to IT Security.

4.6 Use of a password safe/manager is the recommended method to securely store multiple passphrases/passwords, as it is only necessary to remember a single master password.

5. Passphrases/passwords for devices with touchscreen interfaces

5.1 Due to smartphones and tablets having touch-screen interfaces, it is not practical to use a strong password to lock the device. Instead, a numeric password/PIN can be used, if it is at least five characters long.

5.2 See the Securing Computing and Mobile Storage Devices standard for further requirements about Mobile Device security.

6. Biometric alternatives to passphrases/passwords/pins

6.1 Biometric controls such as fingerprint readers and facial recognition are acceptable alternatives to passphrases/passwords/PINs.

7. Multi-Factor authentication

7.1 Where available, it is recommended that users take advantage of multi-factor authentication.

History / Revisions

Date	Action
2024-04-29	*New Standard Approved by: College Information Officer*