



## INFORMATION SECURITY STANDARD #02 Passphrase and Password Protection

### Introduction

1. This document defines standards for the creation and use of passphrases and passwords to protect the [UBC Electronic Information](#) that [Users](#) handle.
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.
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. don't share it or write it down); and
  - c. avoid reusing it for other systems.
4. The Chief Information Officer has issued this document under the authority of Policy SC14, [Acceptable Use and Security of UBC Electronic Information and Systems](#). Questions about this standard may be referred to [information.security@ubc.ca](mailto:information.security@ubc.ca).

### Creating a Passphrase/Password

5. Preferably, use a passphrase with a minimum of 16 characters. If a passphrase is not allowed by a system, use a complex password that contains upper and lower case letters, numbers and symbols. If a password is used then it must be a minimum of 10 characters, but should be 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 thimbles" or "StingersSingPaint").
- 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 "Irmmts7AM!".
- 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. Password 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 turtle phrase	Hx%2Pe2fWE
WhiteCaps2018	trophy.sky.sings.gold	5vE@Pu57^j
12345678ABC	1plusfourbeaches	9#fAaXu7y6tt
GameofThrones	facelessdragonhorse	p39&k1WX3EGxKo
Vanc0uv3r	rainbeachpuddles	gqEWep8#32v2xF8i
2March1976	SingingLionorLamb	Yy6*&u22rB
qwerty1234	Elephantkickscat!.	Jb06MTKS35
M0nk3yABC	MonkeyPatsTiger1	854Htt8EvR
ILoveYou	mammamialetmego	4Qz7cSPgdAB15wLm

### Changing a Passphrase/Password

6. Passphrases/passwords for Campus Wide Login accounts must be changed annually. For all other accounts, it is recommended that passphrases/passwords be changed annually. When changing a passphrase/password:
  - a. do not use the 10 most recent passphrases/passwords that have been used on the same system;



- b. do not use the same passphrase/password for personal accounts and university 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.

### Protecting a Passphrase/Password

7. If a passphrase/password is written down, it must be locked away in a secure, inaccessible location such as a safe.
8. Best practices state that passwords should not be shared for any reason - even with trusted individuals such as supervisors.
9. [University IT Support Staff](#) will never ask for Users' passwords.
10. Do not respond to emails or phone calls requesting passphrases/passwords, even if they appear to be from a trusted source. These requests are often attempts to steal Users' credentials.
11. Passphrases/passwords must be immediately changed if there are suspicions that they could have been compromised and the incident must be reported to UBC Information Security (see the [Reporting Information Security Incidents](#) standard).
12. 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. Refer to the [Password Safe](#) guideline.

### Passphrases/Passwords for Devices with Touchscreen Interfaces

13. 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, as long as it is at least five characters long.
14. See the [Securing Computing and Mobile Storage Devices/Media](#) standard for further requirements regarding mobile device security.

### Biometric Alternatives to Passphrases/Passwords/PINs

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

### Multi-Factor Authentication

16. Where available, it is recommended that Users take advantage of [Multi-Factor Authentication](#).

### Additional Requirements for University IT Support Staff

17. For University IT Support Staff, there are additional requirements around the storage of passphrases/passwords. These requirements are detailed in the [User Account Management](#) standard.

#### Case Study: Why You Shouldn't Share Your Password

A single user ID and password was shared amongst a research lab's personnel. One of these individuals maliciously destroyed some of the data in the account. Since this was a shared account, it was challenging to identify the responsible party.

#### Choosing your Password/PIN for a Mobile Device

A simple password/PIN option is to think of a 5 or 6 letter word and spell it out using the letters on the numeric key pad. Example: HOUSE becomes "46873".



### **Related Documents**

[Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems](#)

[Securing Computing and Mobile Storage Devices/Media standard](#)

[Reporting Information Security Incidents standard](#)

[User Account Management standard](#)

[Securing User Accounts standard](#)

[Password Safe guideline](#)