INFORMATION SECURITY GUIDELINE

Password Safes

Introduction

1. Password Safes (or Password Managers) are computer applications that provide a secure place to store and access the passphrases/passwords for different login environments. Password Safes are simple to use because they can be accessed with a single master passphrase/password.
2. This guideline has been issued by the Chief Information Officer to supplement the Password and Passphrase Protection standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

Master Passwords/Passphrases

3. The master passphrase/password used to protect the Password Safe must be strong; otherwise the security of the safe and all of its contents are at risk. Refer to the Passphrase and Password Protection standard for information on how to design a secure passphrase/password.
4. The master passphrase/password must be changed at least annually.
5. Users are responsible for remembering the master passphrase/password. If it is lost or forgotten, UBC cannot recover or bypass it.

Types of Password Safes

6. Picking a Password Safe can be tricky. Here is a summary of the available options:

Type	Description	Notes
Standalone	These are installed on the desktop or on your mobile device as an application.	With these services, the data is accessible no matter if an internet connection is available or not. However, if the device is lost or the database corrupted, then the only way to recover the data will be through a backup copy.
Web-based	These are accessible through a web browser and are stored online as part of a cloud service.	With these services, the data is not susceptible to database corruption or loss of the device. However if the site is inaccessible or no Internet connection is available, then the passwords will not be accessible.
Web Browser-based	Most web browsers have the ability to “Remember this password” for secure login sites.	Using these services is not recommended. Browsers are subject to constant attack and there are known vulnerabilities that can expose passwords stored in browsers. Many password safes now offer to import the browser passwords lists.
Mixed	Newer services offer a dual environment, with device-based apps that are synched to the cloud.	These combine the benefits of standalone and web-based systems.

Current Leading Password Safes

7. Here are some of the leading Password Safes:

Name	Description	More Information
KeePass	*Available for Windows, Mac OS X and Linux, as well as iOS, Android, Windows and BlackBerry mobile operating systems.* A popular open-source, cross-platform, desktop-based password manager. It stores all passwords in a single database (or a single file) that is protected and locked with one master key. The database can be stored on a cloud drive (e.g. Workspace), which is then accessible across multiple devices. (Recommended)	KeePass Help Center **Type:** Standalone. Can be used as Mixed. **Encryption:** AES-256
LastPass	*Available for Windows, Mac and Linux, as well as iOS, Android and Windows mobile operating systems*. Once the master password has been setup, LastPass will import all saved login credentials (usernames and passwords) from Firefox, Chrome, Internet Explorer, Opera, and Safari. It then prompts for deletion of all of this information from the computer to keep it secure. Supports Multi-Factor Authentication. A premium subscription service is available that includes advanced MFA options, password sharing and encrypted file storage.	LastPass Product FAQ **Type:** Web-based **Encryption:** AES-256
RoboForm	*Available for Windows, Mac, iOS, and Android.* Another password manager, as well as a tool to automatically fill in online forms. RoboForm is RoboForm stores information locally, rather than in the cloud. A subscription service is available, RoboForm Everywhere, which will upload a User's data to the cloud and making it available across multiple platforms.	RoboForm Tutorials **Type:** Standalone. Can be upgraded to Mixed. **Encryption:** AES-256
Dashlane	*Available for Windows, Mac, Linux, Chromebook, iOS and Android, with web extensions for Chrome, IE, Edge, Firefox, Safari, Opera, Linux and Chromebook.* Add or import passwords, or save them as you browse the web. Supports autofill and face ID. A premium subscription service is available that includes unlimited device sync, automatic backup, secure sharing and universal two-factor authentication support.	Dashlane Features **Type:** Mixed **Encryption:** AES-256
1Password	*Apps for Mac, iOS, Windows, Android, and web* A password manager, digital vault, random password generator, form filler and secure digital wallet. 1Password remembers all your passwords for you, and keeps you safe behind the one password that only you know. Monthly fee.	1Password Tour **Type:** Web-based **Encryption:** AES-256

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Password and Passphrase Protection standard