VUB Information Security and Privacy

How To – Password Management

Owner:
Chief Information Security Officer

Contact(s):
ciso@vub.be

Most recent update:
17 March 2020

I. Overview

A “How To …” document provides information and/or hints and tips about a specific Information Security and Privacy (ISP) topic. It does not contain a mandatory standard/guideline. Rather, it provides information about how a standard/guideline can be applied.

It is a ‘living’ document whose quality depends partly on the feedback from its readers/users. The cover page gives the contact email address to which feedback can be sent.

A “How To” document does not follow a formal consultation and approval process.

This How To document deals with password management. It was signed off for publication by the ICT Directorate (DICT).

II. Password Management

Every VUB user is responsible for all actions carried out under his/her VUB username. Consequently, it is very important that your VUB password is protected under all circumstances.

- ⇨ A strong password comprises at least 12 characters. Feel free to use a sentence, including spaces. For example: “I’m the only one who knows my password”.

  If the application does not permit 12 characters, use the maximum number of characters permitted. In that case a combination of upper- and lower-case letters, numbers and special signs (the ‘old’ standard) must be used.

  (The current VUB password can only comprise 8 characters. Preparations are being made to adapt the process that manages the VUB passwords, but this is a time-consuming task and the implementation date is not yet known.)

  You can test the strength of your password, for example on https://howsecureismypassword.net/. Don’t test the password that you want to use here. Instead, enter a similar one (similar in terms of length and structure).

- ⇨ You should change your password at least once a year. Do not re-use old passwords or parts of old passwords. For example, do not change “The horse carries the rider 2018” into “The horse carries the rider 2019”.

- ⇨ Change your password immediately after an incident or a suspected incident. For example:
  - If you lose your laptop or another device that you have used to log in;
  - After an incident involving a central system, whether at the VUB or externally, on which you have (ever) logged in;
  - After your system has been contaminated with a virus and repaired.

- ⇨ Never share your password with others, not even with the VUB Service Desk or your manager. If someone asks for your password, you must refuse.

  If you are away and a colleague has to take over tasks requiring the use of ICT systems to which they don’t have access, arrange for this colleague to be granted the necessary (temporary) access/user's rights. Never 'lend' your colleague your VUB username and password!

You are not permitted to help out a new colleague who does not yet have a username/password by sharing your VUB username and password with them. Request login data for new staff in good time.

A visitor who wants to connect to Wi-Fi but does not have a guest account, may not use your VUB username and password to log into the VUB Wi-Fi network, either. Contact the helpdesk for a guest account. It's best to do this in advance of the visit.

⇨ Do not use your VUB password linked to your VUB username for other services (such as Google mail, Facebook, etc.). You should only use your VUB password with your VUB username.

⇨ Using a single password for various services (Gmail, Facebook, online banking, etc.) is very risky. All it takes is for one service to be hacked and the hacker has access to all your services.

If you use several services for private and professional purposes, remembering all these different passwords can sometimes be an impossible task. Consider using a password manager. Examples of free password managers: LastPass•••|, dashlane and KeePass. Nevertheless, it is best not to store your VUB password here.

⇨ If you want to use the 'remember password' function on your web browser for private or professional purposes (never use it for your VUB password!), activate the option to install a general password on your browser. When you start up your browser, you then simply have to enter this general password once.

This prevents other users logging into your services from your browser by using this function.

⇨ Never write your VUB password down, never save it in a file or never give it in an email.

⇨ If you receive an initial/reset password by email, change it immediately.

⇨ If possible, use Multi-Factor-Authentication (MFA). With this system, as well as entering your username and password, you have to enter a second 'key' to be able to log in. Examples of a second key like this include receiving a text code, receiving a login request in a connected app on your smartphone or copying an app-generated code. This combination alone will grant you access.

By using MFA, you are better protected against improper use of your password.