



# VeraCrypt user guide

Install the software VeraCrypt via the regular way, which is the Software Center in a Windows computer provided by Tampere Universities. For Linux computers, please contact IT Helpdesk. For your own computer, you can install VeraCrypt from VeraCrypt's web [page](#). Please note that your own computer is not secure enough for processing confidential data, for example containing personal data. This guide is for a Windows computer, and you will have to adapt on Linux or Mac.

Restrictions that must be considered before and during the use of Cryptomator:

- 
**PLEASE NOTE:** If the password for the VeraCrypt volume is forgotten, the volume cannot be opened, but all the files in it will be permanently lost.  
 → **When you create a volume and set its password, you must remember it for sure.**
- 
**PLEASE NOTE:** If two users open a volume at the same time in a shared location (such as a project folder) and they both modify the contents of the volume in any way, the latter save of the volume will overwrite the previous save, and changes in the previous save will be lost.  
 → **Each volume may only be modified by one user at a time (for example adding new files or editing files). If more than one user in your project must modify the same volume, agree on taking turns in using it.**

Follow VeraCrypt's [tutorial](#) and find some supplementary instructions below for some of the steps.

Use cases:

- For storing confidential data:
  - VeraCrypt is secure enough for storing also especially sensitive data, such as the Special categories of data specified in the Article 9 of the GDPR. Select the suitable storage location according to the regular guidelines available in the intranet.
  - Notice below the special instructions regarding USB devices.
- For making a backup of data:
  - VeraCrypt is secure enough for making a backup of also especially sensitive data, such as the Special categories of data specified in the Article 9 of the GDPR.
  - Plan a good storage for the backup. As a rule, a backup should be in a different storage system than where the data is currently. For example, if the data is currently in a project folder (S drive), for the backup you should prepare storage in a folder synced from Teams or in a USB drive (memory stick or a larger drive).
  - If you plan to use a USB drive, plug it to your computer and find out what the disk drive letter is. Notice below the special instructions regarding USB devices.

If you want to store especially sensitive data, such as the Special categories of data specified in the Article 9 of the GDPR, on an external USB device, you will have to first encrypt the device with software BitLocker. That process is very simple. Search the instructions for that from intranet with the keyword BitLocker.

In *STEP 5*, select the location where you want to create the VeraCrypt volume. For a USB drive it is a new disk drive letter, perhaps D:.

In *STEP 9*, set the volume size to large enough. If you use a USB drive and you do not want to store any other data there, you can make the volume as large as the free space on the drive.

In *STEP 10*, set a strong password for the volume according to the guidance of the software. **If the password is forgotten, the volume cannot be opened, and the files contained in it will be permanently lost.**

In *STEP 11*, move the mouse randomly within the window until the meter at the bottom of the window goes all the way to the right side.

Now the volume is ready for use. Open the volume starting from the *STEP 13* and select a letter other than A, B, P, or S as VeraCrypt's virtual disk drive.

A new virtual disk drive (M: in VeraCrypt's tutorial) will appear on your computer.

You can now start storing data to the new virtual disk drive.

Close the VeraCrypt volume by clicking *Dismount* when you have stopped accessing the data in the volume.

When you want to open a VeraCrypt volume, follow the steps of the tutorial starting from *STEP 13*.