VeraCrypt user guide

1. Install the software

Install the software VeraCrypt via the regular way, which is the Software Center in a Windows computer provided by Tampere Universities. If you need to store classified information in an approved manner, i.e. in accordance with the usage policy published by Traficom, do not install the latest version available at the Software Center (at 1.25.9) and ask IT Helpdesk to share a Traficom-approved version on your workstation (1.25.7). For more information, see the page Cryptography solutions approved by Traficom's NCSA-FI.

If you need Veracrypt for a Mac computer, contact IT Helpdesk. This manual is for Windows computers and on Mac computers you will need to adapt this. For Linux computers, VeraCrypt is not available yet.

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.

2. Restrictions

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

⚠
- **PLEASE NOTE:** If the password for the VeraCrypt volume is forgotten and lost, the volume cannot be opened, but all the files in it will be permanently lost.
  ➔ Write down the password on a physical note in full or in part. More guidelines available on the page Take control of your passwords by the National Cyber Security Center. Store this note in a secure place. Write down the information in a way that makes it impossible for outsiders to determine the services that the passwords are for or the user if the note goes missing.

⚠
- **PLEASE NOTE:** If two users open a volume at the same time in a shared location (such as a group directory) 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.

3. Use cases

3.1. Store 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.

3.2. Make 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 group directory (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.

3.3. Encrypt a USB device with BitLocker

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.

4. Create a VeraCrypt volume

If the largest file you need to store in a volume encrypted with VeraCrypt is less than 4 GB in size, create a store in a new file according to the instructions in section 4.1. If you need to be able to store a file larger than 4 GB, use the instructions in section 4.2 to create a store by encrypting an entire partition (partition).

4.1. Create a volume in a file

Follow the VeraCrypt tutorial and find some supplementary instructions below for some of the steps.

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. **More guidelines available on the page Take control of your passwords by the National Cyber Security Center. Write down the password on a physical note in full or in part. Store this note in a secure place. Write down the information in a way that makes it impossible for outsiders to determine the services that the passwords are for or the user if the note goes missing. If the password is forgotten and lost, 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.

When you reach the *Volume Created* screen in VeraCrypt, the volume is ready to use, and you can continue to use it according to the instructions in chapter 0.

4.2. Create a volume in a partition

To store more than 4 GB files, you need to create a VeraCrypt volume by encrypting a full partition (partition). This can be done easily with a USB drive or stick according to the following instructions. This instruction assumes that the USB disk used is empty. So make sure the disk is empty, or if you are sure you can, apply this guide according to your situation. If necessary, contact IT Helpdesk.

Follow the VeraCrypt tutorial and find some supplementary instructions below for some of the steps.

In the Veracrypt tutorial in *STEP 3 VeraCrypt Volume Creation Wizard*, select *Encrypt a non-system partition/drive*.

Under *STEP 4 Volume Type*, select *Standard VeraCrypt volume*.

Under *STEP 5 Volume Location*, select the USB device and then select the partition on it.

In *STEP 10*, set a strong password for the volume according to the guidance of the software. **More guidelines available on the page Take control of your passwords by the National Cyber Security Center. Write down the password on a physical note in full or in part. Store this note in a secure place. Write down the information in a way that makes it impossible for outsiders to determine the services that the passwords are for or the user if the note goes missing. If the password is forgotten and lost, the volume cannot be opened, and the files contained in it will be permanently lost.**

In step *Large Files,* select Yes*.*

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. If you select *Quick Format*, the creation of the volume is a lot faster.

When you reach the *Volume Created* screen in VeraCrypt, the volume is ready to use, and you can continue to use it according to the instructions in chapter 0.

5. Use the volume

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.

The next step takes place differently depending on the type of volume:

- If you created the volume in a file according to chapter 4.1, proceed as instructed from *STEP 14*.
- If you created the volume in a partition according to chapter 4.2, choose *Select Device* in *STEP 14*, then click the partition you encrypted, and then continue from the *STEP 16*.

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

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

If you want to make a backup of files encrypted with Boxcryptor, make sure that you copy the files from the Boxcryptor virtual drive X:. In other words, do not copy files from the storage space where the encrypted files are (for example the network drive S:), because when copied, the files would not be decrypted with Boxcryptor and they would remain encrypted with Boxcryptor also in your backup.

Boxcryptor will stop working in October 2023 when our Boxcryptor license expires, and then the files encrypted with Boxcryptor become useless. The name of the files encrypted with the Boxcryptor have ".bc" at the end when you look at them outside of the Boxcryptor virtual drive X:. After copying files to VeraCrypt virtual drive, check that it does not contain files with “.bc” in the end of the filename.

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

6. If Windows reports the space available on the S disk to be too small

If you have a problem that you are trying to save a file to an S disk, but the program gives an error message that there is not enough space, then it may be that Windows incorrectly reports the available space on the S disk as too small. A proper solution is being developed for this.

Here’s how to get around the problem:

1. Start TUNI VPN unless you're on any campus. Open File Explorer, click on the S: drive to see the names of your group directories.
2. Click on the Windows icon at the bottom left, type cmd and press enter to start the command line window.
3. Type the command “subst v: s:\group_directory” in which you place the name of your group directory. In this case, a new disk drive V is created on your computer, and it shows the content of your group directory. You can replace the letter V with any free letter you want (not these: C, P, S). Finally, enter the command “exit” and the command line window will close.
4. To turn off the drive V you created, type “subst v: /d”.
5. Start using the new drive V: whenever you want to use that group directory. In this case, Windows can correctly tell all programs how much space is available in the group directory.
6. The specification in step 3 is not valid after you have logged out or restarted your computer. If you want this definition, i.e. disk drive V: always done on your computer when you check in, do this:
    - Reopen command line window according to step 2 and type the following commands: “cd C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup” and “edit subst.cmd” and “notepad subst.cmd”.
    - In this case, you should open Notepad application, where you create a new text file. Type the same command you gave in step 3 of this guide as the contents of the file. Close Notepad and save the file. Finally, enter the command “exit” and the command line window will close.
    - If you want to edit this file later, you can do it with these same commands.
    - If you want to delete this task definition for your login, open the command line window according to the instructions in section 2 and enter the commands “del C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\subst.cmd” and “exit”.