BREDGAR PARISH COUNCIL (BPC)

Encryption Work Instruction

This Work Instruction was reviewed by the Full Council at its meeting held on August 29th 2018

1) **Scope**

   This work instruction is intended for staff and councillors of Bredgar Parish Council.

2) **Objective**

   To ensure compliance with the General Data Protection Regulations BPC requires all staff and councillors to store all council data within encrypted folders on BPC or their own computer equipment.

3) **Hardware and Software Encryption Solutions**
   Recent computers that are delivered with Windows 10 Professional OS often have a hardware device within them: a "Trusted Platform Module" or TPM. This is a chip on your computer's motherboard that helps enable tamper-resistant full-disk encryption without requiring extremely long pass phrases. Conversely, if you were to pay for an upgrade to Windows 10 Pro OS, using an existing laptop or desktop computer, it is quite likely that there will be no TPM present and so using Bit Locker becomes more complicated to set up, albeit not impossible.

   Staff or Councillors who have Windows 10 Pro operating system on their computer and whose computer has a TPM may wish to use the Bit Locker. Microsoft provide instructions for the use and installation of Bit Locker on the Internet.

   Staff or councillors without Windows 10 Pro or a computer with TPM may wish to use the 'Open Source' encryption program VeraCrypt. This software enables the creation of an encrypted folder, within which all council data can be securely held. Full documentation of VeraCrypt software can be found in the Internet. This procedure is based on the online VeraCrypt Documentation Beginners Guide and this should be used if more information is required.

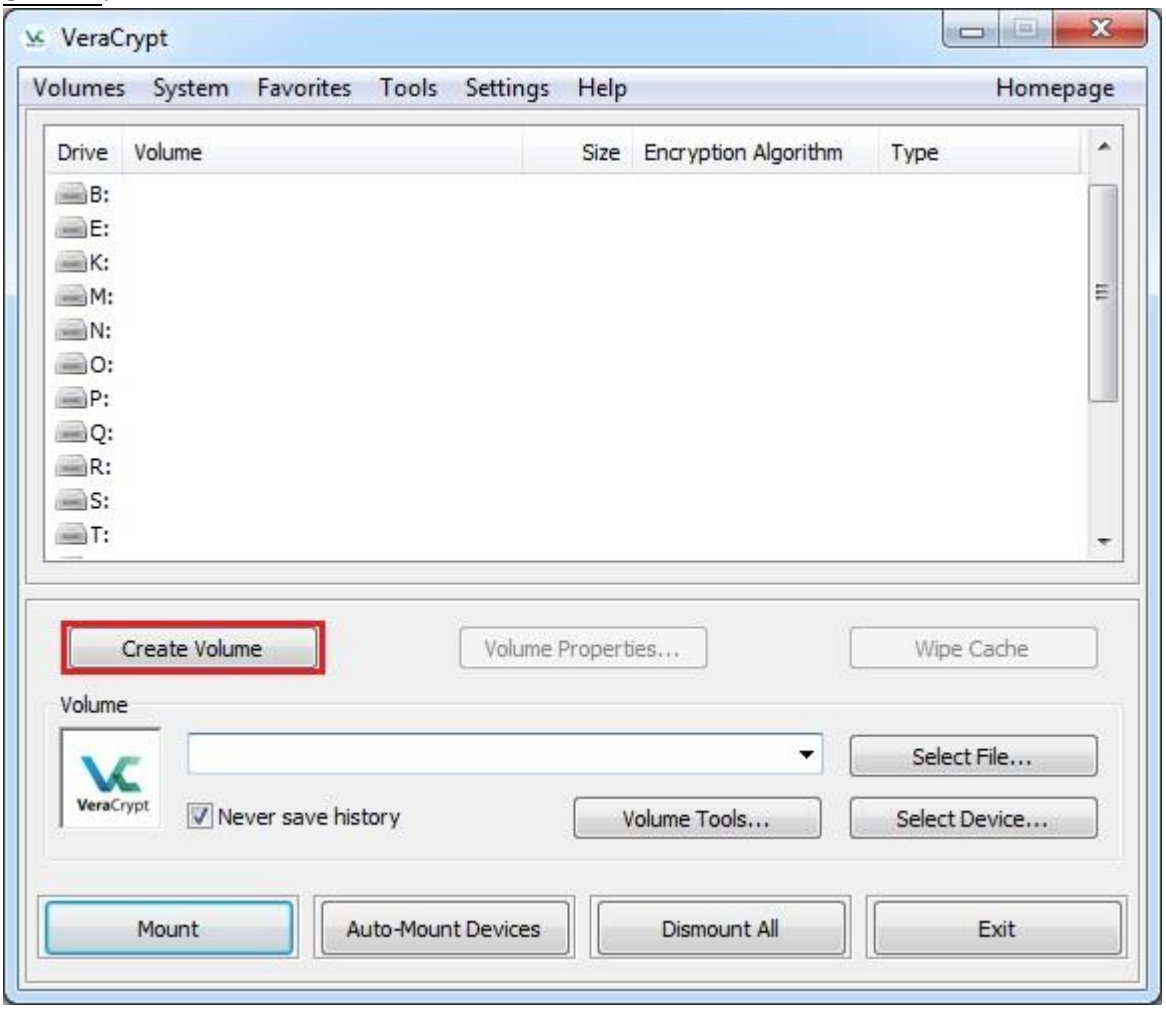
4) **Procedure**

   a) Read the VeraCrypt documentation.
   b) Create and Use a VeraCrypt Container (see Beginners Tutorial online).

      STEP 1:
      If you have not done so, download and install VeraCrypt. Then launch VeraCrypt by

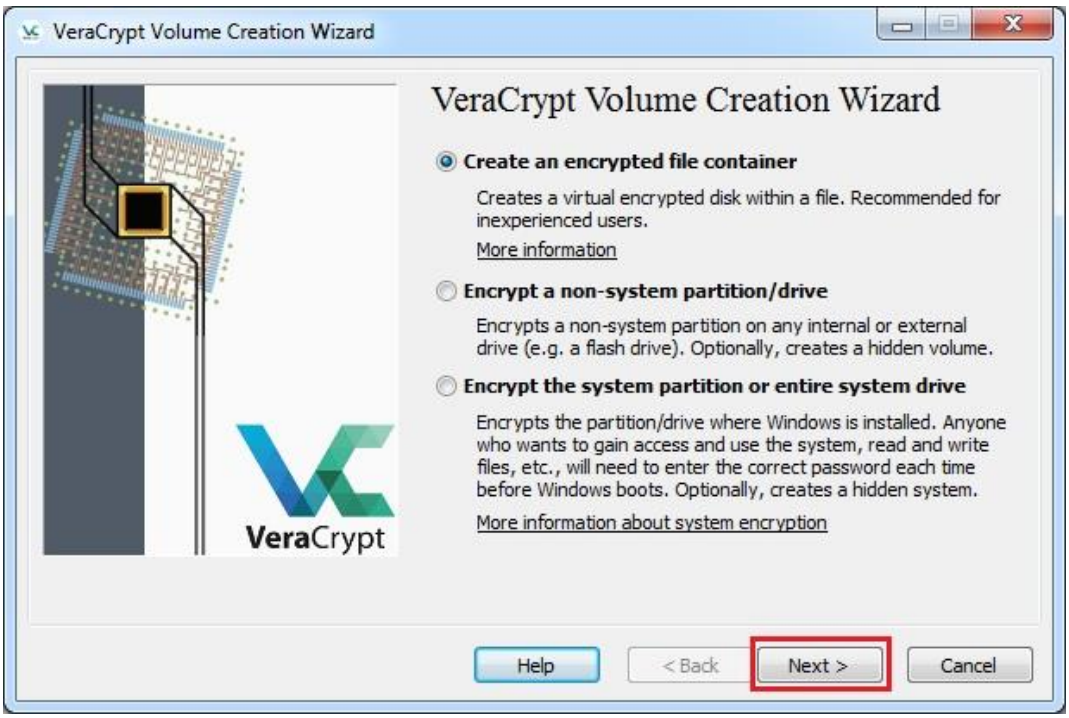
double-clicking the file VeraCrypt.exe or by clicking the VeraCrypt short-cut in your Windows Start menu.

STEP 2:



The main VeraCrypt window should appear. Click **Create Volume** (marked with a red rectangle for clarity).

STEP 3:



The VeraCrypt Volume Creation Wizard window should appear.

In this step you need to choose where you wish the VeraCrypt volume to be created. A VeraCrypt volume can reside in a file, which is also called container, in a partition or drive. In this tutorial, we will choose the first option and create a VeraCrypt volume within a file.

As the option is selected by default, you can just click **Next**.

Note: In the following steps, the screenshots will show only the right-hand part of the Wizard window.

STEP 4:

In this step you need to choose whether to create a standard or hidden VeraCrypt volume. In this tutorial, we will choose the former option and create a standard VeraCrypt volume.

As the option is selected by default, you can just click **Next**.

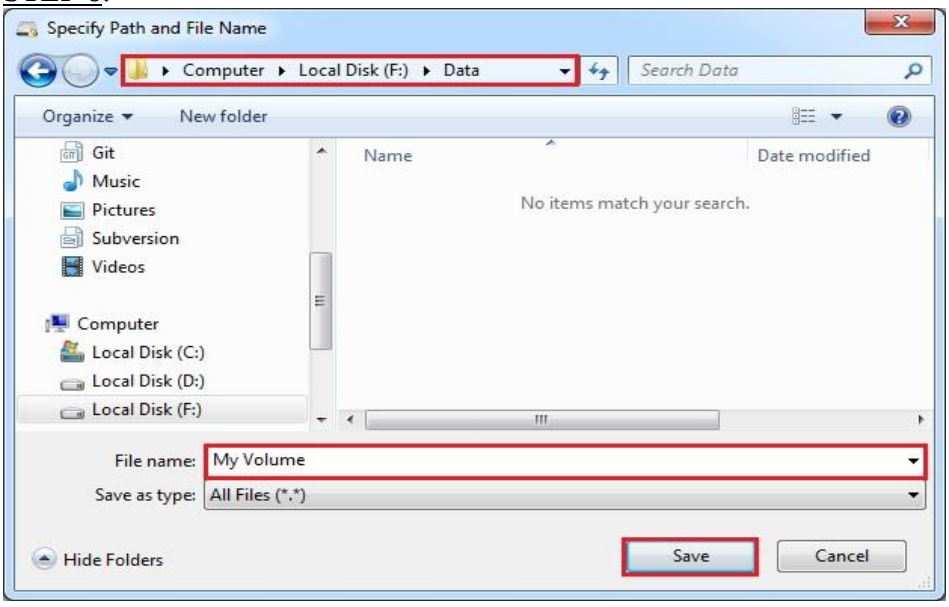
STEP 5:

In this step you have to specify where you wish the VeraCrypt volume (file container) to be created. Note that a VeraCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

Click **Select File**.

The standard Windows file selector should appear (while the window of the VeraCrypt Volume Creation Wizard remains open in the background).

STEP 6:



In this tutorial, we will create our VeraCrypt volume in the folder F:*Data*\ and the filename of the volume (container) will be *My Volume* (as can be seen in the screenshot above). You may, of course, choose any other filename and location you like (for example, on a USB memory stick). Note that the file *My Volume* does not exist yet – VeraCrypt will create it.

Note: Substitute '*My Volume*' with an appropriate name for your Bredgar Parish Council container – for example *BPC* or '*Bredgar PC'* or similar.

IMPORTANT: Note that VeraCrypt will *not* encrypt any existing files (when creating a VeraCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be *lost*, *not* encrypted). You will be able to encrypt existing files (later on) by moving them to the VeraCrypt volume that we are creating now.*

Select the desired path (where you wish the container to be created) in the file selector. Type the desired container file name in the **Filename** box.

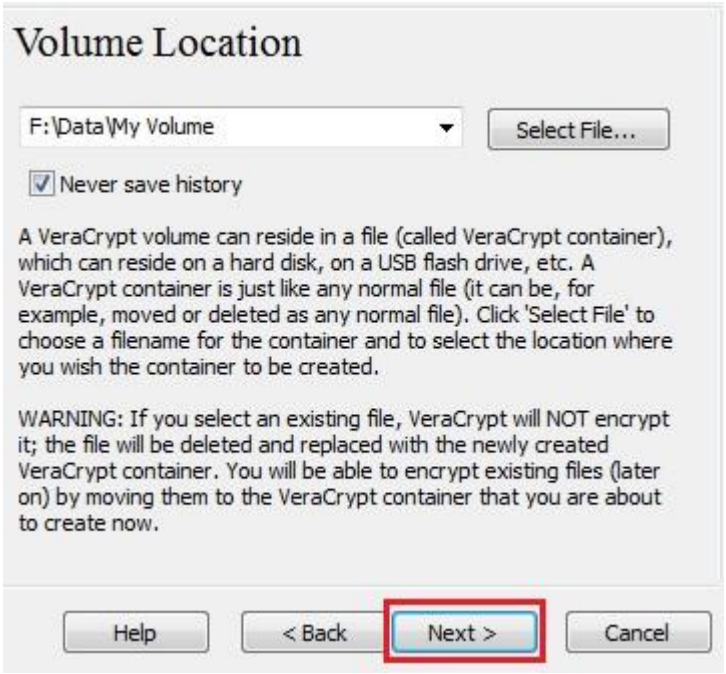
Click **Save**.

The file selector window should disappear.

In the following steps, we will return to the VeraCrypt Volume Creation Wizard.

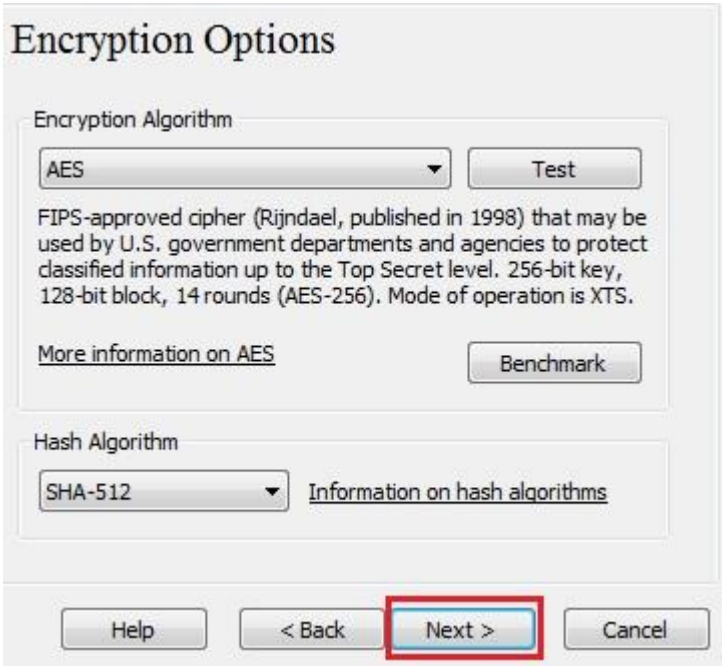
* Note that after you copy existing unencrypted files to a VeraCrypt volume, you should securely erase (wipe) the original unencrypted files. There are software tools that can be used for the purpose of secure erasure (many of them are free).

STEP 7:



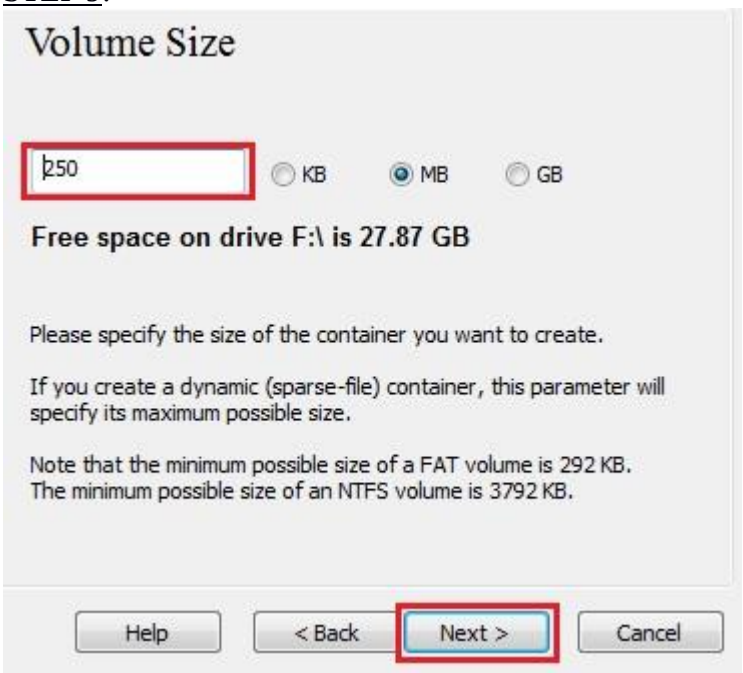
In the Volume Creation Wizard window, click **Next**.

STEP 8:



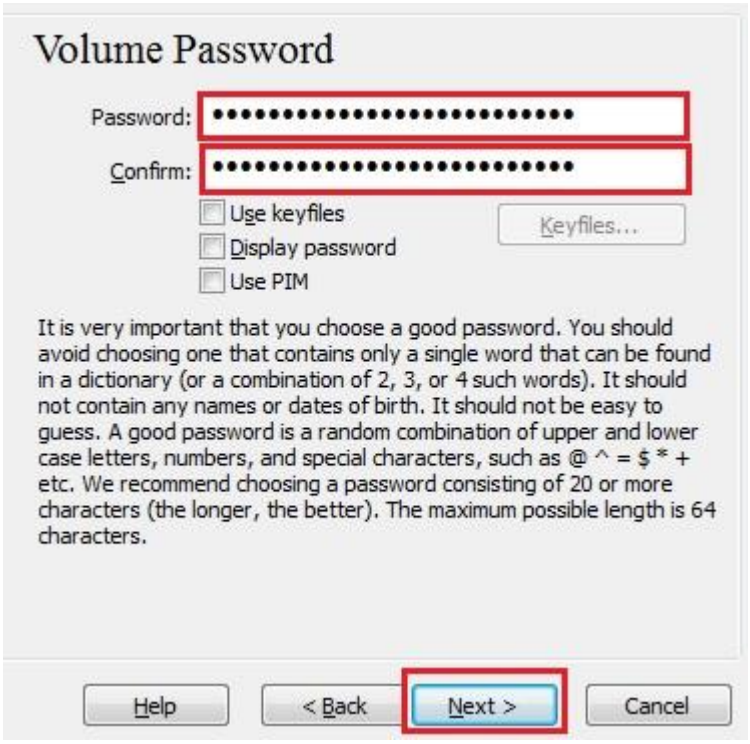
Here you can choose an encryption algorithm and a hash algorithm for the volume. If you are not sure what to select here, you can use the default settings and click **Next**.

STEP 9:



Here we specify that we wish the size of our VeraCrypt container to be 250 megabyte. You may, of course, specify a different size. After you type the desired size in the input field (marked with a red rectangle), click **Next**.

STEP 10:

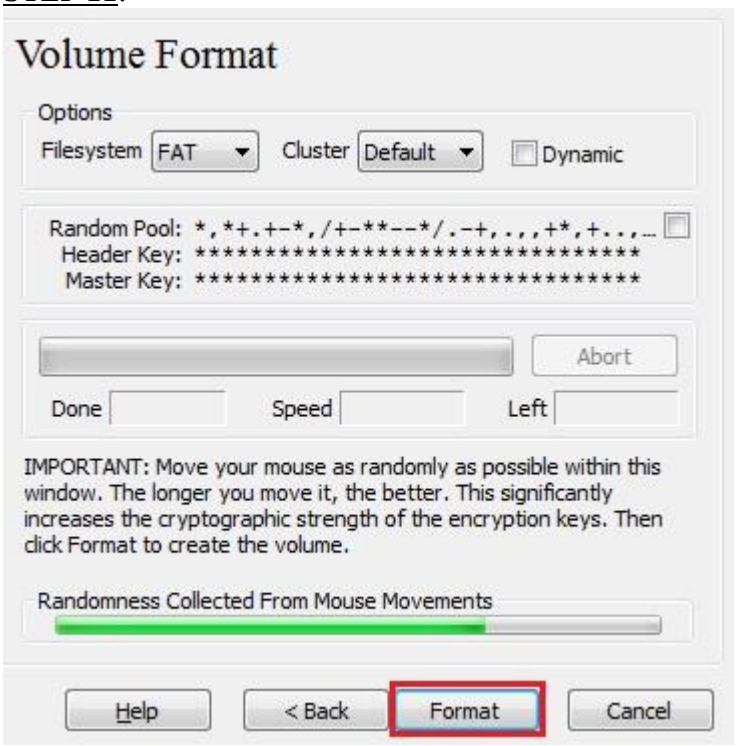


This is one of the most important steps. Here you have to choose a good volume password. Read carefully the information displayed in the Wizard window about what is considered a good password.

After you choose a good password, type it in the first input field. Then re-type it in the input field below the first one and click **Next**.

Note: The button **Next** will be disabled until passwords in both input fields are the same.

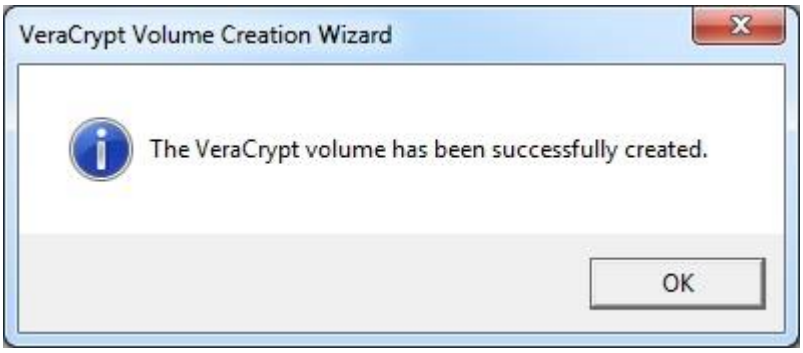
STEP 11:



Move your mouse as randomly as possible within the Volume Creation Wizard window at least until the randomness indicator becomes green. The longer you move the mouse, the better (moving the mouse for at least 30 seconds is recommended). This significantly increases the cryptographic strength of the encryption keys (which increases security).

Click **Format**.

Volume creation should begin. VeraCrypt will now create a file called *My Volume* in the folder F*:\Data* (as we specified in Step 6). This file will be a VeraCrypt container (it will contain the encrypted VeraCrypt volume). Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box will appear:



Click **OK** to close the dialog box.

STEP 12:

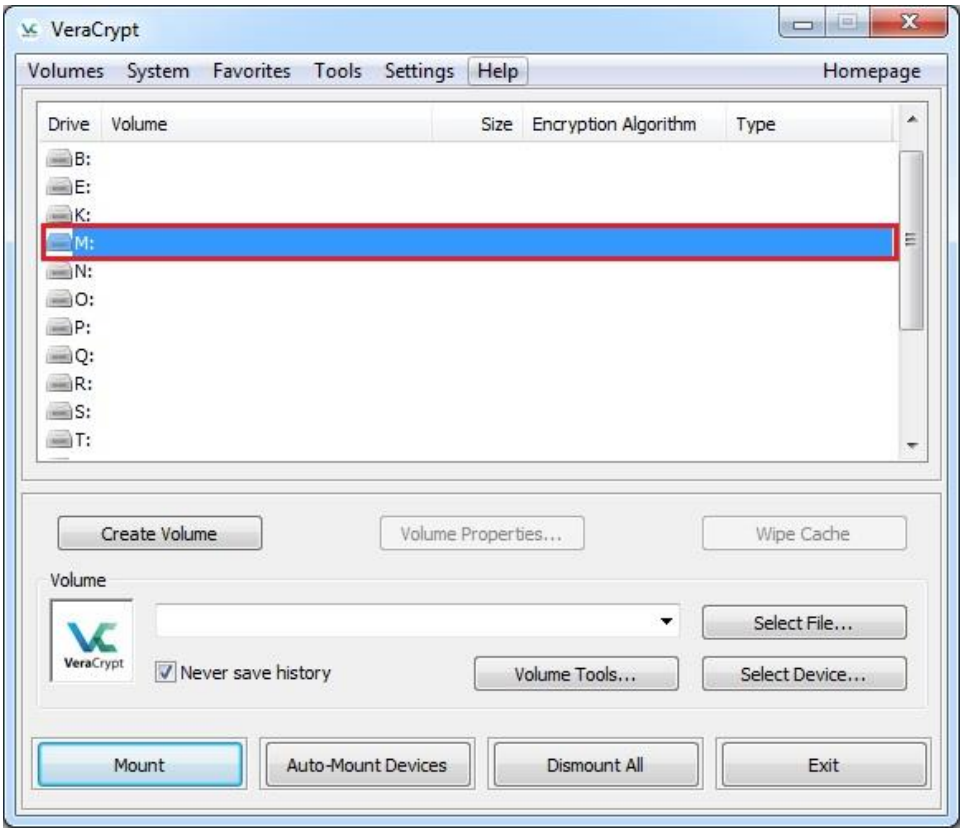
We have just successfully created a VeraCrypt volume (file container). In the VeraCrypt Volume Creation Wizard window, click **Exit**.

The Wizard window should disappear.

In the remaining steps, we will mount the volume we just created. We will return to the

main VeraCrypt window (which should still be open, but if it is not, repeat Step 1 to launch VeraCrypt and then continue from Step 13.)

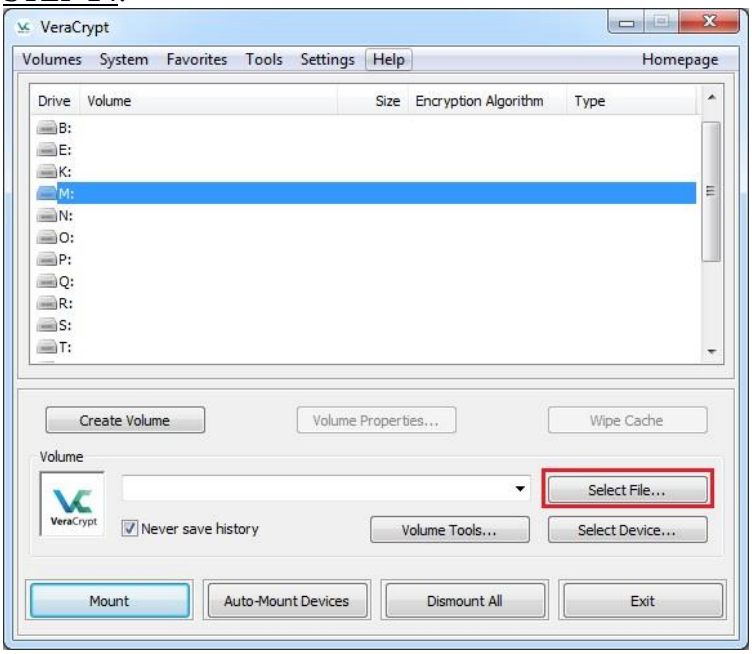
STEP 13:



Select a drive letter from the list (marked with a red rectangle). This will be the drive letter to which the VeraCrypt container will be mounted.

Note: In this tutorial, we chose the drive letter M, but you may of course choose any other available drive letter.

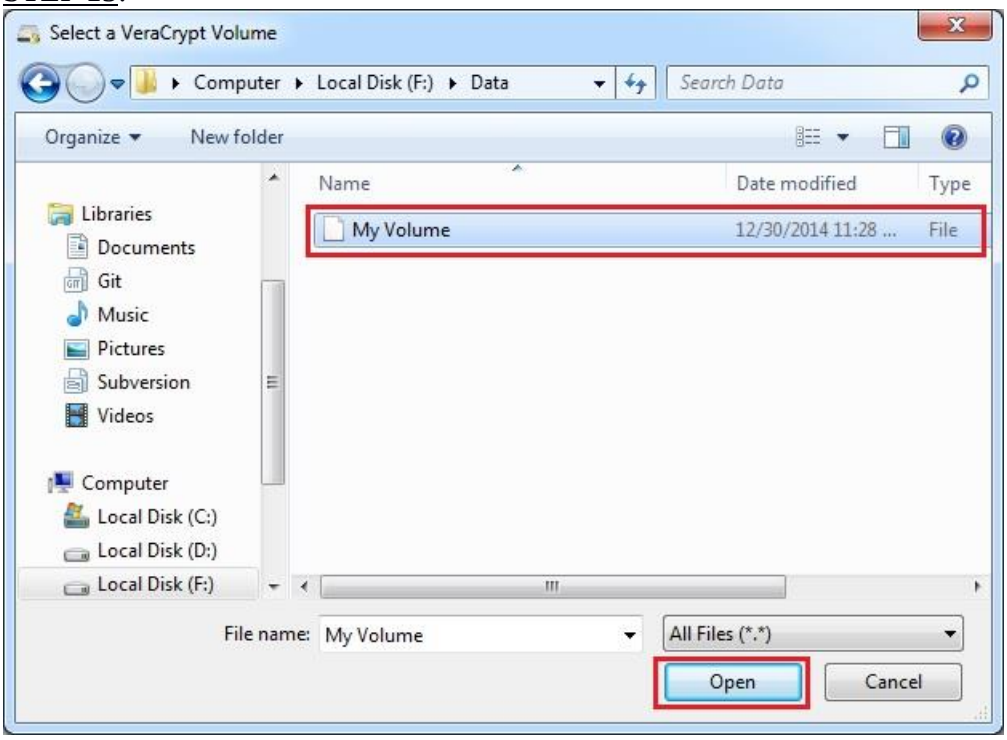
STEP 14:



Click **Select File**.

The standard file selector window should appear.

STEP 15:

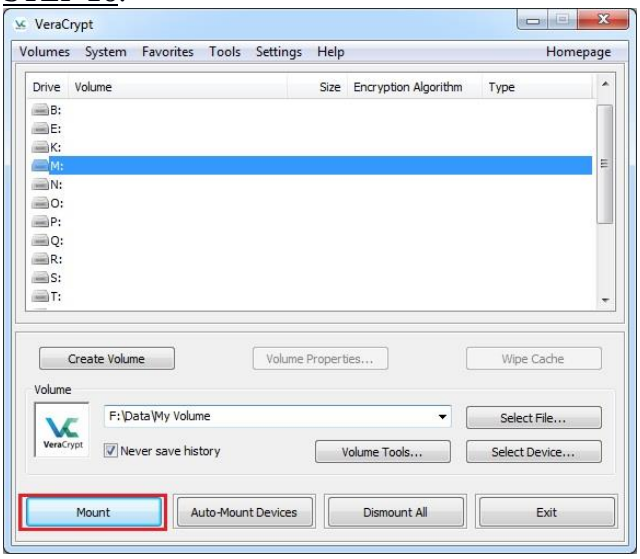


In the file selector, browse to the container file (which we created in Steps 6-12) and select it. Click **Open** (in the file selector window).

The file selector window should disappear.

In the following steps, we will return to the main VeraCrypt window.

STEP 16:



In the main VeraCrypt window, click **Mount**. Password prompt dialog window should appear.

STEP 17:

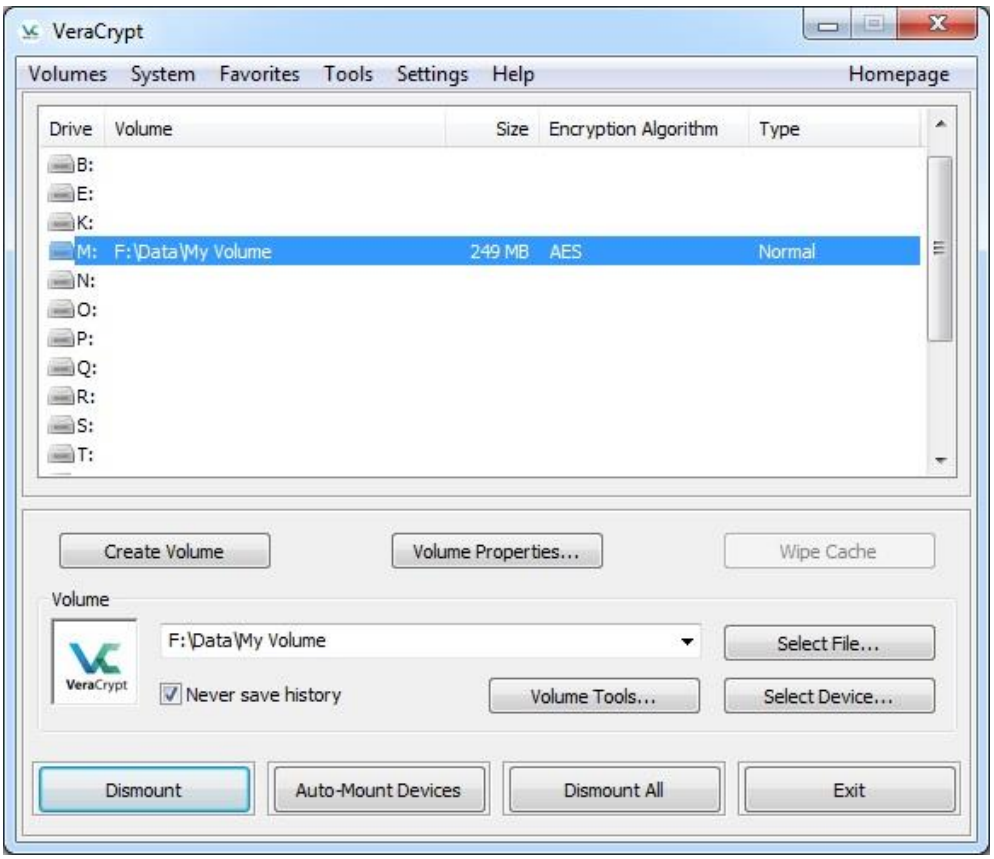
Type the password (which you specified in Step 10) in the password input field (marked with a red rectangle).

STEP 18:

Select the PRF algorithm that was used during the creation of the volume (SHA-512 is the default PRF used by VeraCrypt). If you don't remember which PRF was used, just leave it set to "autodetection" but the mounting process will take more time. Click **OK** after entering the password.

VeraCrypt will now attempt to mount the volume. If the password is incorrect (for example, if you typed it incorrectly), VeraCrypt will notify you and you will need to repeat the previous step (type the password again and click **OK**). If the password is correct, the volume will be mounted.

FINAL STEP:



You have just successfully mounted the container as a virtual disk M:

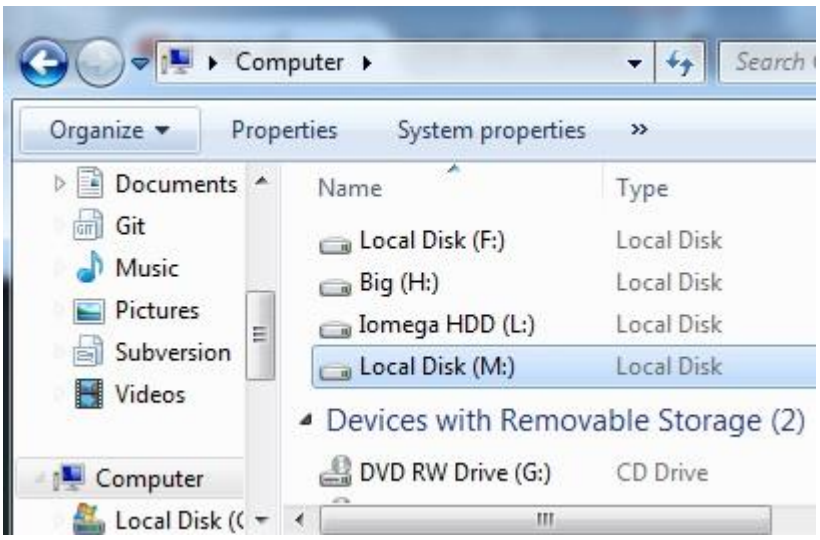
The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.

If you open a file stored on a VeraCrypt volume, for example, in media player, the file will be automatically decrypted to RAM (memory) on the fly while it is being read.

Important: Note that when you open a file stored on a VeraCrypt volume (or when you write/copy a file to/from the VeraCrypt volume) you will not be asked to enter the password again. You need to enter the correct password only when mounting the volume.

You can open the mounted volume, for example, by selecting it on the list as shown in the screenshot above (blue selection) and then double-clicking on the selected item.

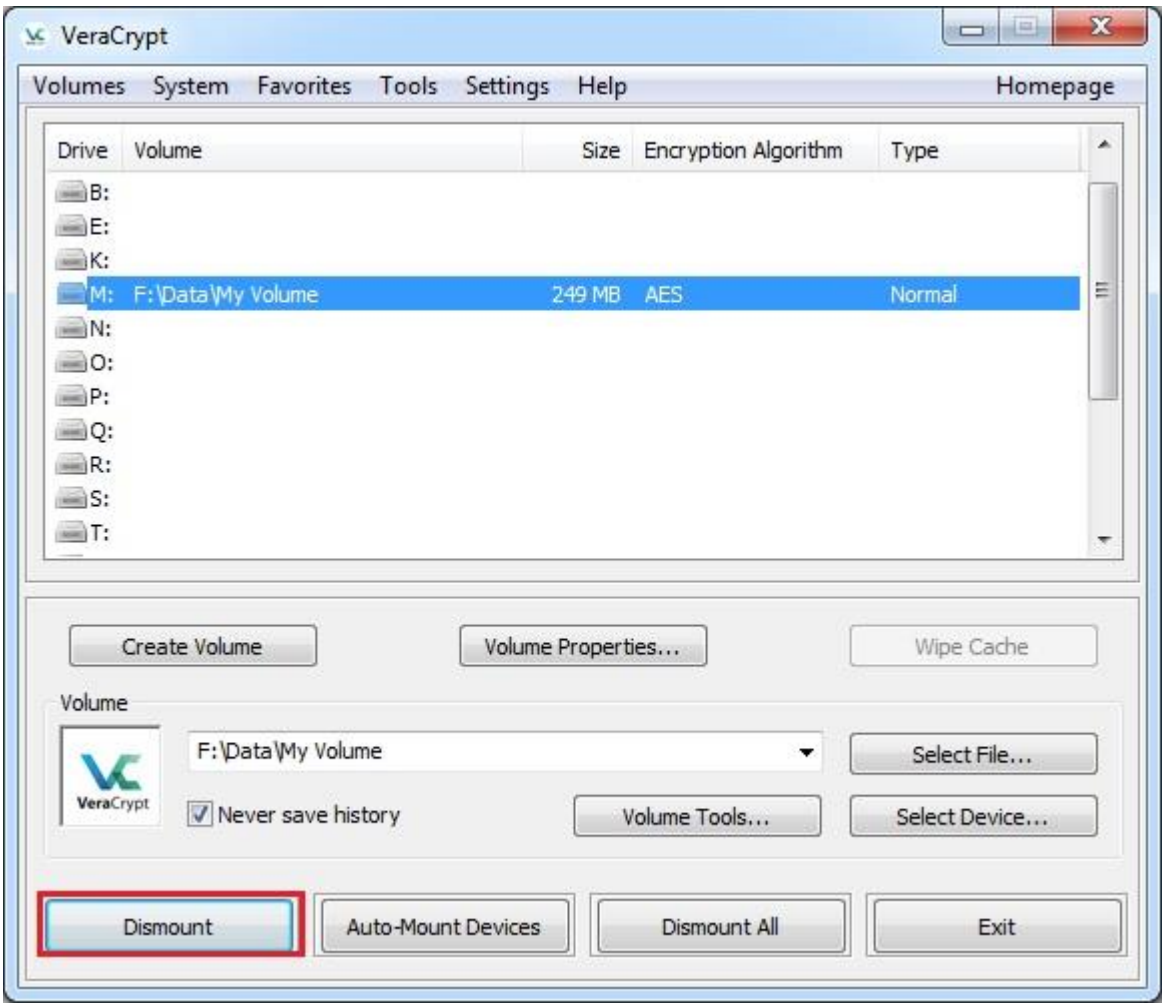
You can also browse to the mounted volume the way you normally browse to any other types of volumes. For example, by opening the '*Computer*' (or '*My Computer*') list and double clicking the corresponding drive letter (in this case, it is the letter M).



You can copy files (or folders) to and from the VeraCrypt volume just as you would copy them to any normal disk (for example, by simple drag-and-drop operations). Files that are being read or copied from the encrypted VeraCrypt volume are automatically decrypted on the fly in RAM (memory). Similarly, files that are being written or copied to the VeraCrypt volume are automatically encrypted on the fly in RAM (right before they are written to the disk).

Note that VeraCrypt never saves any decrypted data to a disk – it only stores them temporarily in RAM (memory). Even when the volume is mounted, data stored in the volume is still encrypted. When you restart Windows or turn off your computer, the volume will be dismounted and all files stored on it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted (without proper system shut down), all files stored on the volume will be inaccessible (and encrypted). To make them accessible again, you have to mount the volume. To do so, repeat Steps 13-18.

If you want to close the volume and make files stored on it inaccessible, either restart your operating system or dismount the volume. To do so, follow these steps:



Select the volume from the list of mounted volumes in the main VeraCrypt window (marked with a red rectangle in the screenshot above) and then click **Dismount** (also marked with a red rectangle in the screenshot above). To make files stored on the volume accessible again, you will have to mount the volume. To do so, repeat Steps 13-18.

5) **Donations**

The VeraCrypt software is free to use but donations are accepted to support ongoing development.