

# HOW to QUICKLY and PERMANENTLY SANITIZE ANY DRIVE (SSD, USB thumb drive or standard hard drive)

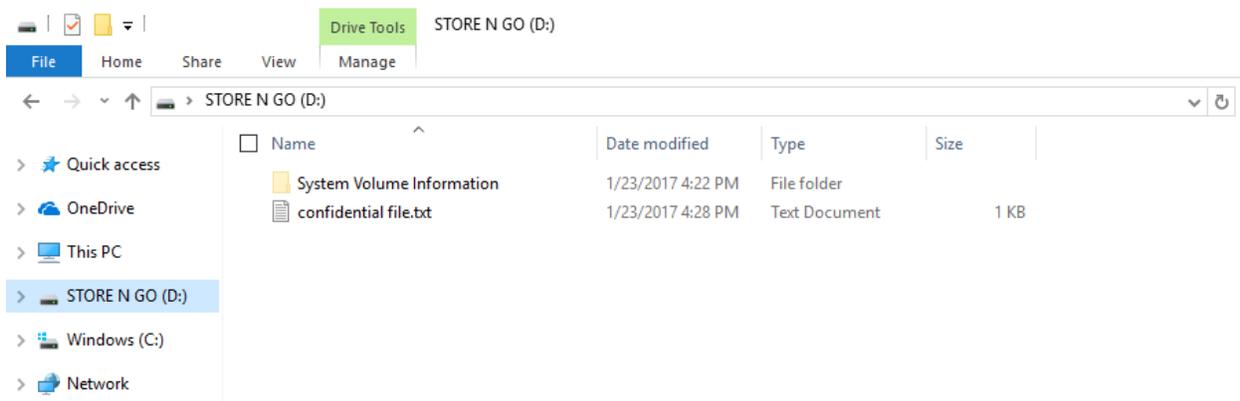
This document will show how to sanitize media and ensure no data can be recovered. We will do this by doing four steps.

1. We will use the Windows tool BitLocker to encrypt the drive.
2. We will then format the drive.
3. We will then re-encrypt the drive one final time. By re-encrypting it a second time, the encryption key from Step 1 will be overwritten, rendering the encrypted data from the first encryption unrecoverable, and leaving the drive with random, meaningless data.
4. We will format the drive one more time. This will leave the drive ready for future reuse.

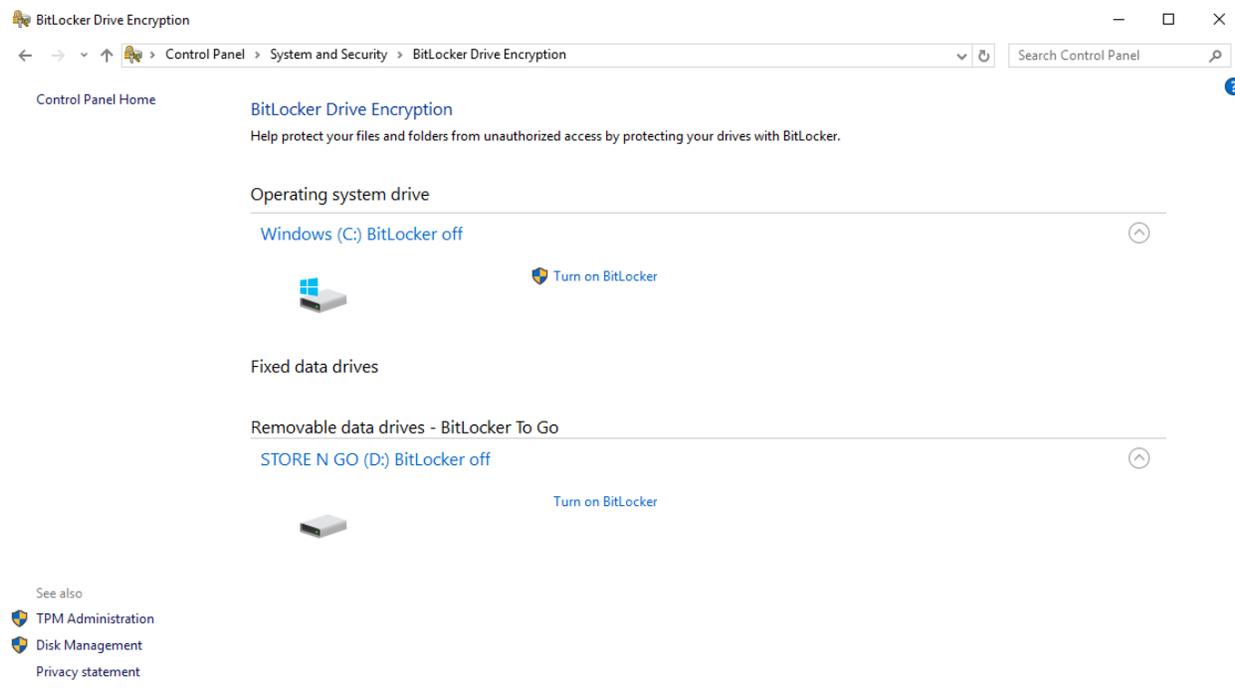
## Step 1.

Connect the drive to your system and enable BitLocker on it.

In this example, we have a thumb drive with some confidential data on it. We want to ensure that no one can ever recover this data. You can see this in Windows Explorer. In this example, the drive is D:.

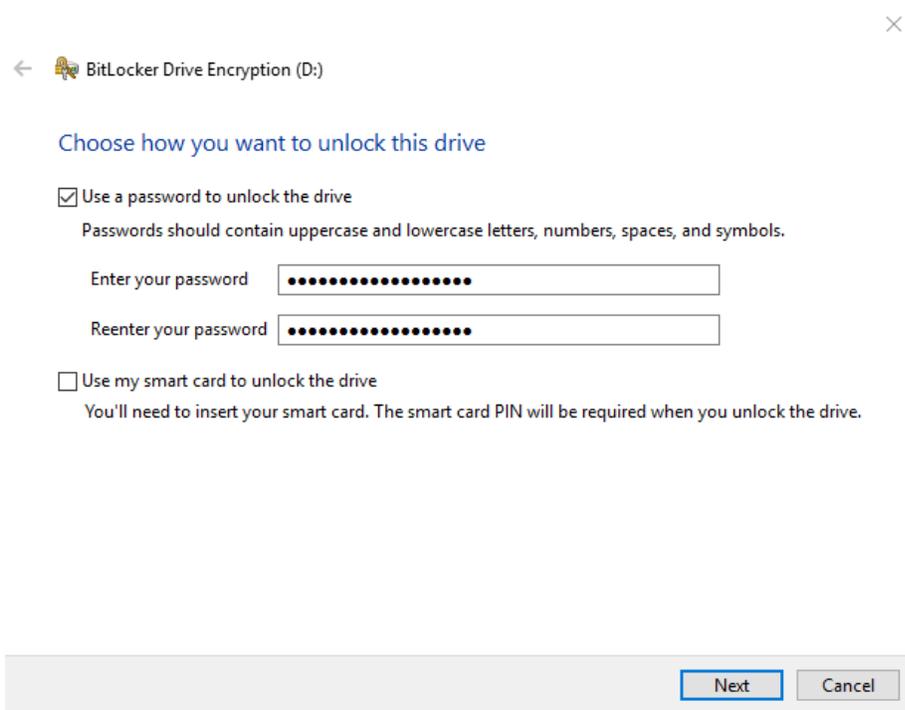


Open BitLocker (Click *Search* and run bitlocker or Control Panel\System and Security\BitLocker Drive Encryption). Note: you may need administrative privileges to run BitLocker.

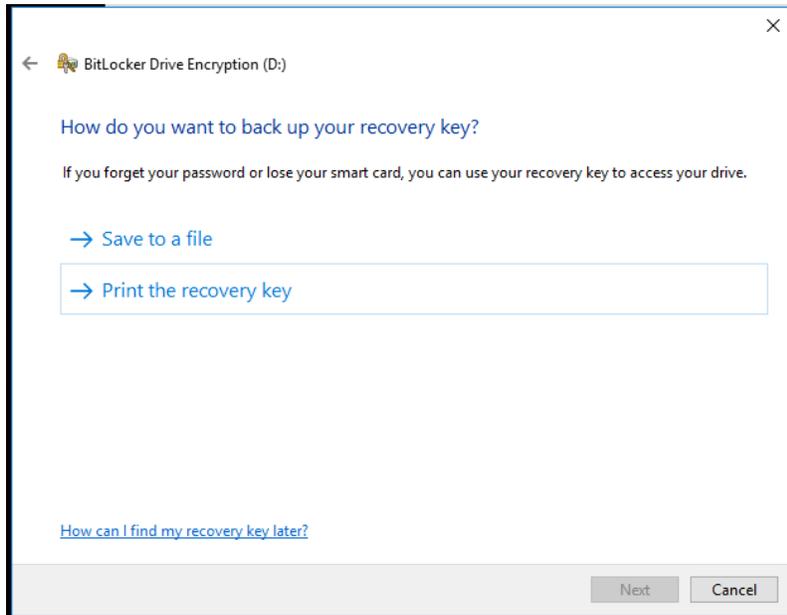


Click *Turn on BitLocker* (Do not do this on your C: drive unless you want to encrypt your C: drive)

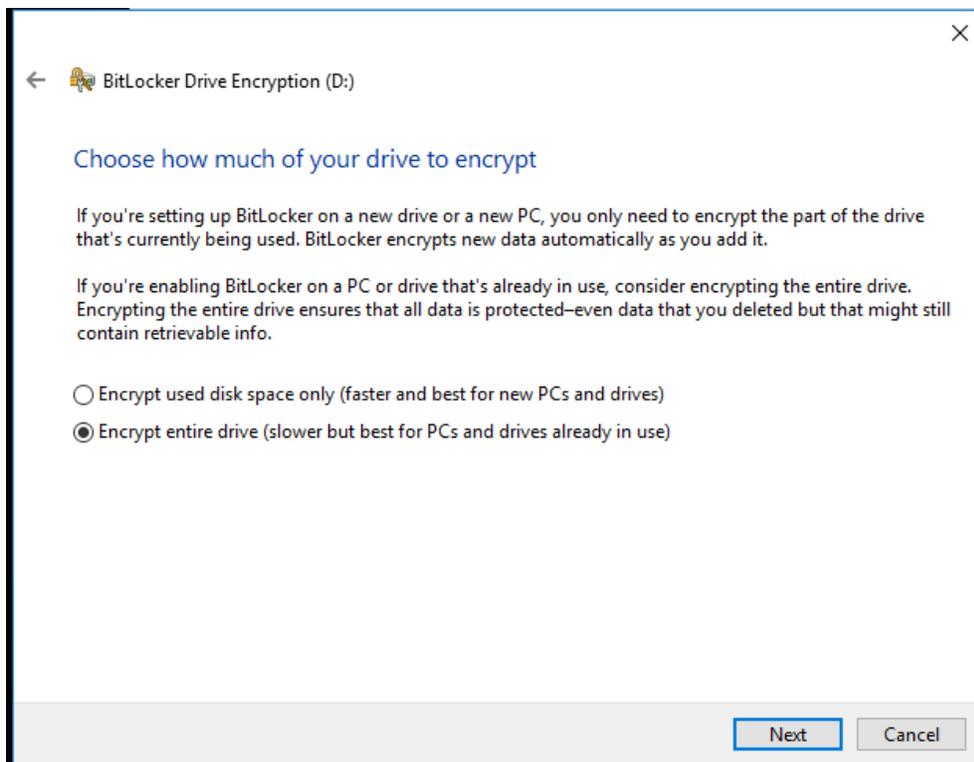
Set up a password to unlock the drive. Use any random characters. You will not need to remember this password, so it can be anything.



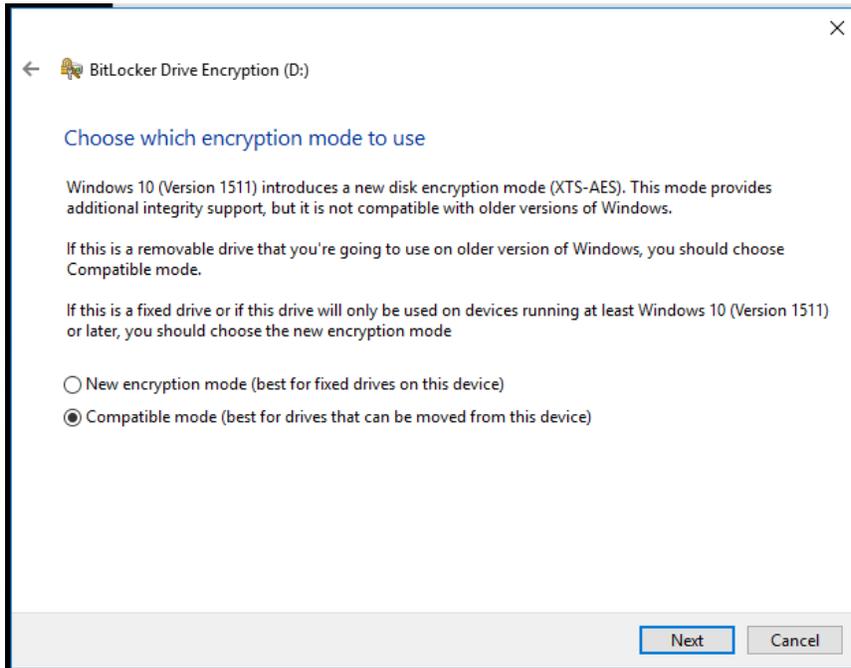
When prompted to save or print the recovery key either save it to a location other than the media you are sanitizing or print it out and shred the paper. I suggest saving it to an alternate location, then deleting the file after it is saved.



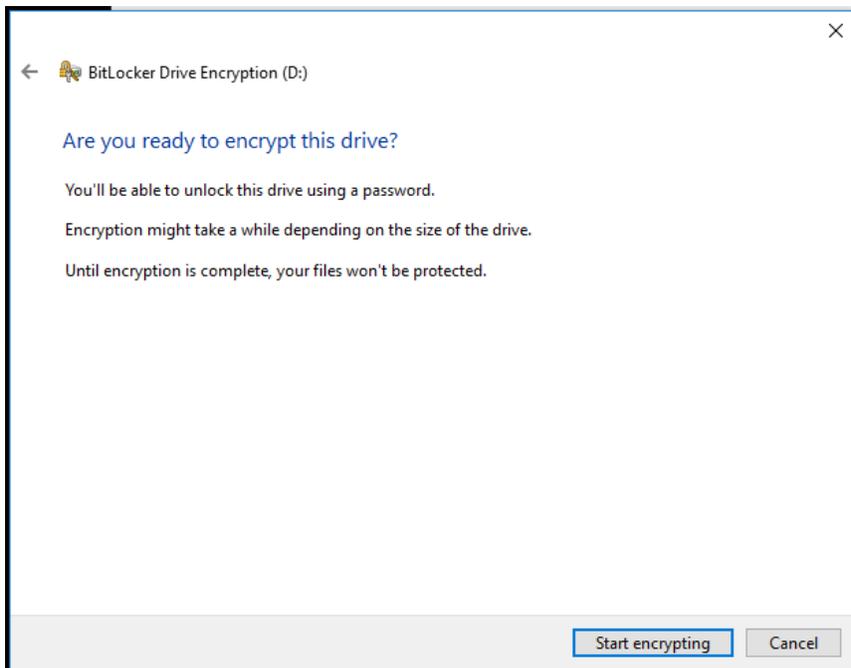
When prompted to Choose how much of your drive to encrypt, choose to encrypt the entire drive. This will ensure that any deleted files or data remaining on the drive are also encrypted.



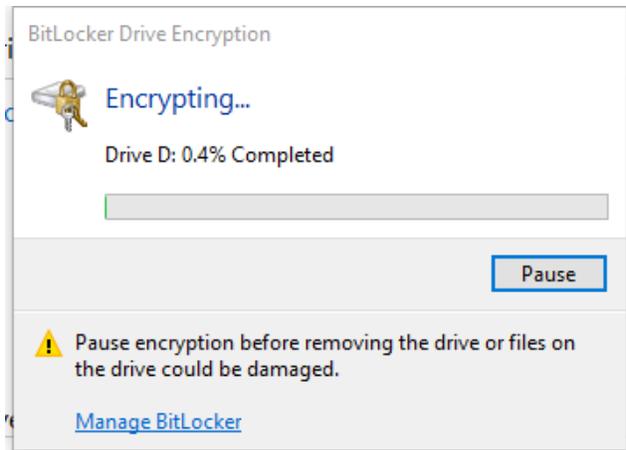
If running this on Windows 10 operating system, you will be prompted to choose an encryption mode. Choose either mode, it doesn't matter since we will be formatting this drive shortly.



Click *Start encrypting* when to start the encryption process.

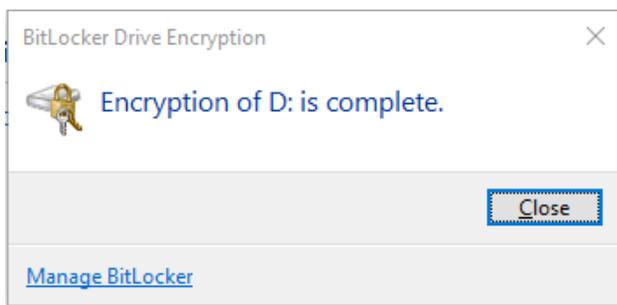


Wait for the encryption to complete.



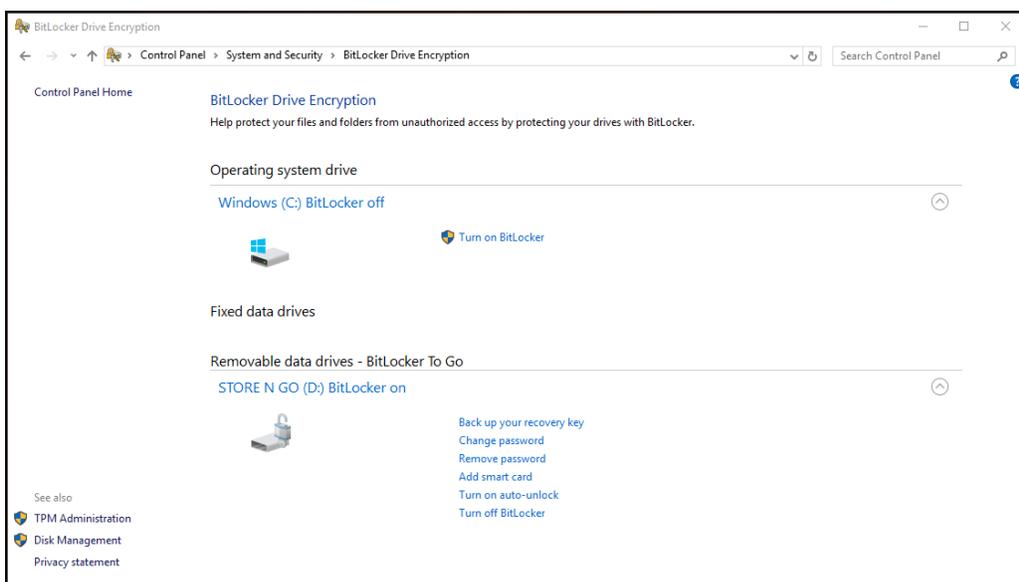
Note that this can take quite a while.

Once finished, you will get the following message:



You can close BitLocker.

You will now see that BitLocker is on:

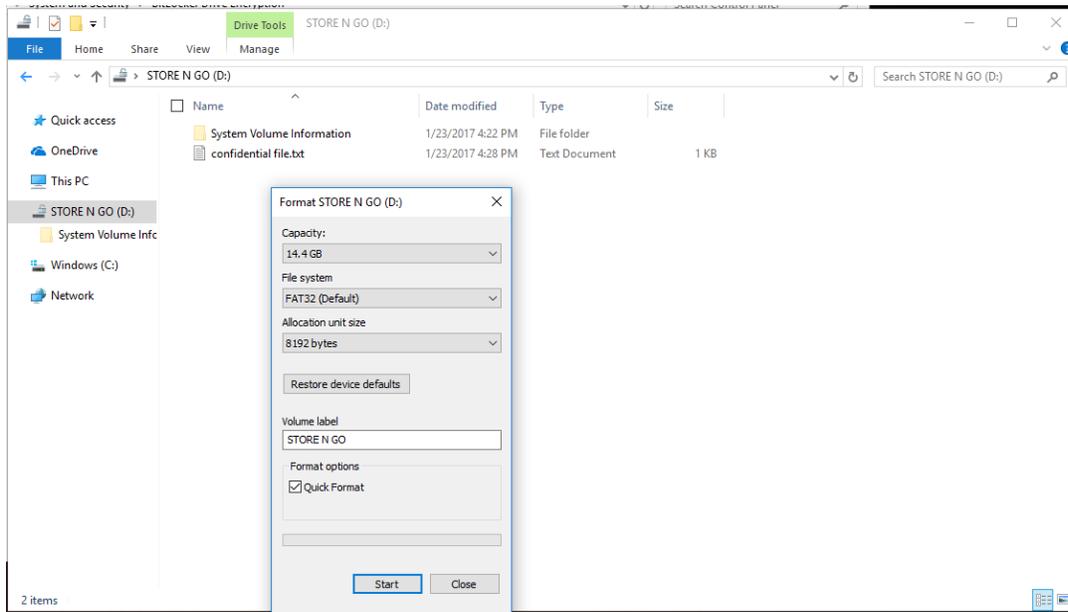


## Step 2:

Format the drive.

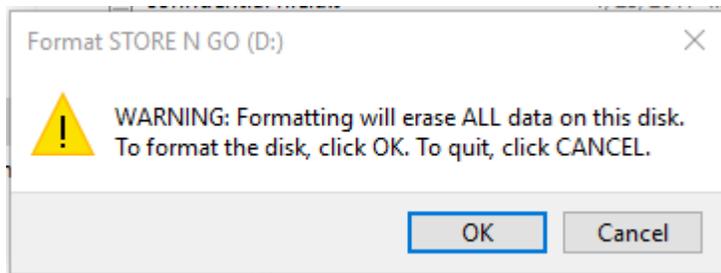
Open Windows explorer, right click on the drive (D: in this case) and choose format.

You can choose a Quick Format if you like.

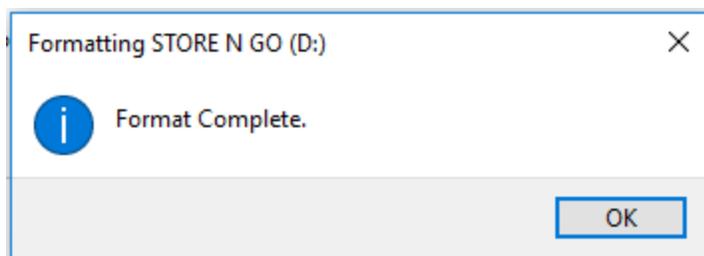


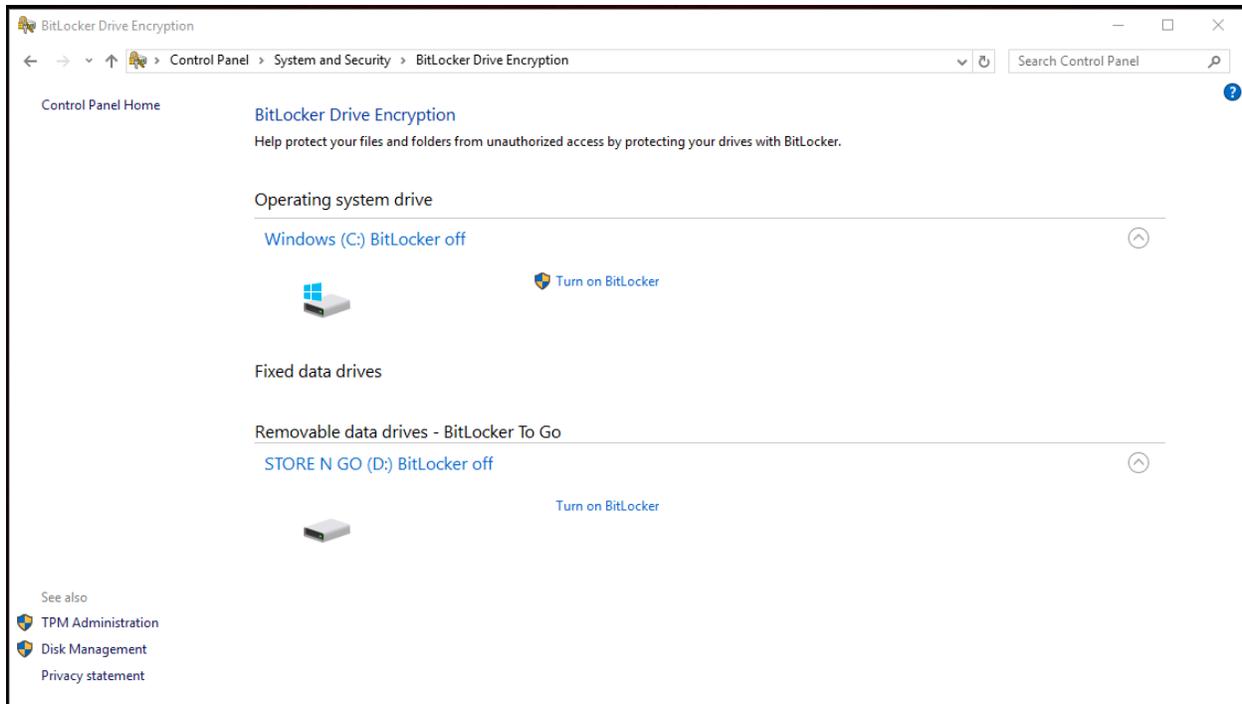
Click *Start*.

When prompted with the warning that formatting the disk will erase all data on the disk, choose *OK*.



Once the format has completed you will see that the BitLocker is now off again.





### Step 3:

Now, to permanently destroy the encryption key, turn BitLocker back on.

Go through the same steps we did previously.

- Set a unique password to unlock the device (pick a different password than you picked previously). Any random characters will suffice.
- Save or print the recovery key (then delete the file or shred the paper)
- You can choose to Encrypt only used space to speed up this second encryption process (we are really only interested in overwriting the encryption key).
- If you want to leave the drive encrypted, you will need to choose which encryption mode to use. If you are going to format the drive again after this process, it doesn't matter (this only applies to Windows 10).
- Start the encryption process (The encryption process should complete much faster this time).

### Step 4:

Format the drive one more time. Again a quick format is fine.

At this point the drive has now been overwritten with encrypted data and the original encryption key has been destroyed. Any data on the drive is unrecoverable, random data. The drive can now be reused or redeployed as necessary.

