# 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.

Ą	BitLocker Drive Encryption			- 0	×
÷	- 🔿 👻 🛧 褬 > Control Par	nel > System and Security > BitLocker Drive Encryption 🗸 💆	Search Control P	anel	Q
	Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.			0
		Operating system drive			
		Windows (C:) BitLocker off		$\bigcirc$	
		Turn on BitLocker			
		Fixed data drives			
		Removable data drives - BitLocker To Go			
		STORE N GO (D:) BitLocker off		$\bigcirc$	
		Turn on BitLocker			
<ul> <li></li> <li><th>See also TPM Administration Disk Management Privacy statement</th><th></th><th></th><th></th><th></th></li></ul>	See also TPM Administration Disk Management Privacy statement				

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.

		$\times$
$\leftarrow$	🏘 BitLocker Drive Encryption (D:)	
	Choose how you want to unlock this drive	
	Use a password to unlock the drive	
	Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.	
	Enter your password	
	Reenter your password	
	Use my smart card to unlock the drive	
	You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive	£.
	Next Can	cel

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.

÷	🏘 BitLocker Drive Encryption (D:)	×
	How do you want to back up your recovery key?	
	If you forget your password or lose your smart card, you can use your recovery key to access your drive.	
	$\rightarrow$ Save to a file	
	→ Print the recovery key	
	How can I find my recovery key later?	
	Next Cance	

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.

	×
←	RitLocker Drive Encryption (D:)
	Choose how much of your drive to encrypt
	If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.
	If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might still contain retrievable info.
	Encrypt used disk space only (faster and best for new PCs and drives)
	Encrypt entire drive (slower but best for PCs and drives already in use)
	Next Cancel

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.

	×
←	Real BitLocker Drive Encryption (D:)
	Choose which encryption mode to use Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides
	additional integrity support, but it is not compatible with older versions of Windows. If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.
	If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode
	○ New encryption mode (best for fixed drives on this device)
	Ocmpatible mode (best for drives that can be moved from this device)
	Next Cancel

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

		×
÷	🏘 BitLocker Drive Encryption (D:)	
		ľ
	Are you ready to encrypt this drive?	
	You'll be able to unlock this drive using a password.	
	Encryption might take a while depending on the size of the drive.	
	Until encryption is complete, your files won't be protected.	
	Start encrypting Cancel	

Wait for the encryption to complete.



Note that this can take quite a while.

Once finished, you will get the following message:

BitLocker Drive Encryption	×
Encryption of D: is complete.	
	<u>C</u> lose
Manage BitLocker	

#### You can close BitLocker.

You will now see that BitLocker is on:

Real BitLocker Drive Encryption				_	1 X
← → × ↑ 🏘 > Control P	anel > System and Security > BitLocker Dr	rive Encryption	~ Ö	Search Control Panel	٩,
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from	unauthorized access by protecting your drives with BitLocker.			•
	Operating system drive				
	Windows (C:) BitLocker off			$\bigcirc$	
		💖 Turn on BitLocker			
	Fixed data drives				
	Removable data drives - BitLo	cker To Go			
	STORE N GO (D:) BitLocker of	n		$\bigcirc$	
See also TPM Administration Disk Management Privacy statement	â	Back up your recovery key Change password Remove password Add smart card Turn on auto-unlock Turn off BitLocker			

## Step 2:

Format the drive.

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

🚔 | 🕑 📙 👳 | Drive Tools STORE N GO (D:) File Home Share View Manage 0 → \* ↑ 🚔 > STORE N GO (D:) ✓ ひ Search STORE N GO (D:) م Name Date modified Туре Size 📌 Quick access System Volume Information 1/23/2017 4:22 PM File folder a OneDrive confidential file.txt 1/23/2017 4:28 PM Text Document 1 KB 💻 This PC Format STORE N GO (D:) × 🚔 STORE N GO (D:) System Volume Infc Capacity: 14.4 GB 🏪 Windows (C:) File system Network FAT32 (Default) Allocation unit size 8192 bytes  $\sim$ Restore device defaults Volume label STORE N GO Format options Quick Format Start Close 8--

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.



Ą	BitLocker Drive Encryption			_	$\times$
<	- 🔿 👻 🛧 🍖 > Control Pane	al → System and Security → BitLocker Drive Encryption	~ Ū	Search Control Panel	P
	Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.			?
		Operating system drive			
		Windows (C:) BitLocker off		$\bigcirc$	
		Turn on BitLocker			
		Fixed data drives			
		Removable data drives - BitLocker To Go			
		STORE N GO (D:) BitLocker off		$\bigcirc$	
		Turn on BitLocker			
\$	See also TPM Administration Disk Management Privacy statement				

## 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.

🏘 BitLocker Drive Encryptic	on		_		×
← → ~ ↑ 🏘 > Co	ontrol Panel > System and Security > BitLocker Drive Encryption	5 V	Search Control Panel		م
Control Panel Home				2	
	Operating system drive				
	Windows (C:) BitLocker off		$\bigcirc$	)	
	V Turn on BitLocker				
	Fixed data drives				
	Removable data drives - BitLocker To Go				
	STORE N GO (D:) BitLocker off		$\bigcirc$	)	
	Turn on BitLocker				
See also					
TPM Administration					
💡 Disk Management					
Privacy statement					
·					
➡   🗹 📑 <del>-</del>   File Home Share	Drive Tools         STORE N GO (D:)           View         Manage		_		× ~ ?
$\leftarrow$ $\rightarrow$ $\checkmark$ $\bigstar$ $\blacksquare$ $\rightarrow$ ST(	ORE N GO (D:)	ڻ <i>ب</i>	Search STORE N GO (D:	:)	Q
- Quick access	Name Date modified Type Size				
T QUICK access					

$\leftarrow \rightarrow \land \downarrow \blacksquare \diamond$ st	ORE N GO (D:)				~ Ū	Search STORE N GO (D:)	Q
1 Ouishaaaaa	Name ^	Date modified	Туре	Size			
Y Quick access	System Volume Information	1/24/2017 8:29 AM	File folder				
a OneDrive							
💻 This PC							
STORE N GO (D:)							
System Volume Infc							
🏪 Windows (C:)							
💣 Network							
1 item							