

HOW TO ENCRYPT ELECTRONIC MEDIA USING BITLOCKER

Please follow the below instructions to encrypt electronic media using BitLocker.

1. Insert the electronic media device into your computer hard drive. The below dialog box will appear.



2. The **'Encrypt this drive using BitLocker Drive Encryption'** option is checked by default. The drive will be read-only until encryption is complete.

3. The 'Use a password to unlock the drive' option is checked by default.

- a) Enter your password twice. Passwords must meet the established password authentication standard. <u>Click here</u> for details.
- b) Click 'Next.'

÷	RitLocker Drive Encryption (D:)	×
	Choose how you want to unlock this drive	
	 Some settings are managed by your system administrator. 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 Cance	4

4. Check this box: 'Encrypt used disk space only (faster and best for new PCs and drives).'

a) Click 'Next.'

÷	A BitLocker 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

5. Click 'Start encrypting.'

			×
÷	🎭 BitLocker Drive Encryption (D:)		
	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

a) The below dialog box will appear indicating the 'Completed' status.

BitLocker Drive Encryption				
Ŕ	Encrypting Your drive will be read-only until encryption is complete.			
	Drive D: 1.7% Completed			
	Pause			
A P d	ause encryption before removing the drive or files on the rive could be damaged.			
N	lanage BitLocker			

Future Use:

1. Insert the electronic media device into your computer hard drive. Depending upon the configuration of your computer, the following dialog box may or may not appear.

File File Explorer File Home Share View View View View	Move Copy Delete Rename New Tests - Pro	Popen → Select all Edit Select none Select all	□ × misc
Clipboard	Organize New	Open Select	
$\leftarrow \rightarrow \land \uparrow$		~ X	٩
	Insert disk X		
			Unlock drive D: This drive is BitLocker-protected.

2. Enter the password you created in **Step 3a**.

BitLocker (D:)		
Enter password to unlock this driv	e.	
	<u>م</u>	
More options		
	Unlock	

If you encounter any problems or forget your encryption password call the OIT Helpdesk at (504) 671-5500.

Disclaimer: Any software made available to Delgado Community College students, employees, or affiliates for use on personal devices is provided "as is" without warranty or guarantee of any kind, either expressed or implied, to the intention and/or effectiveness of performing the desired functions. Persons installing and using this software do so at their own risk and are advised to ensure that the software provided is compatible with existing software and hardware on their personal devices. By accepting this software, the user acknowledges that in no event shall Delgado Community College (DCC) and/or the Office of Information Technology (OIT) be liable to the user or any third party for any special, punitive, incidental, indirect or consequential damages of any kind, or any damages whatsoever, including, without limitation, those resulting from loss of use, data or profits, whether or not DCC and/or OIT have been advised of the possibility of such damages, and/or on any theory of liability, arising out of or in connection with the use of this software. Further, DCC and OIT do not provide technical support or troubleshooting for issues related to personal device hardware and/or software. Any questions or issues regarding personal devices should be directed to the manufacturer or vendor.