Electronic Discovery at the Butler County Prison

This document describes the processes and requirements for providing an inmate with electronic discovery at the Butler County Prison.

Prison administration recognizes that most information is now created, stored, and processed electronically. Accordingly, discovery in criminal cases is often provided to defense attorneys in digital format.

This institution will accommodate a defendant's need to review the discovery in his or her case, but it must also take steps to ensure the integrity and confidentiality of the information provided. In furtherance of this goal, the Butler County Prison has developed the following standards and procedures for attorneys who wish to provide electronic discovery to their clients.

Discovery Desktops

Beginning on 4/19/2024, the prison will provide secure desktop computers for inmates to review discovery. The desktop computers will be available on each pod, and inmates will need to request a ___ hour time slot each day between 7:30 AM and 7:30 PM to review discovery.

The discovery will be placed on encrypted flash drives, which will be in the custody of the prison, except for the time when the inmate is using one of the desktops.

Types of Media

USB flash drives are the preferred media for storing electronic discovery. Flash drives come in capacities ranging from 16 gigabytes to one terabyte (1000 gigabytes). Requirements for flash drives are listed below:

- Only flash drives with a USB Type A Connector (see Figure 1) will be accepted at the prison.
- Flash drives must be formatted with the Microsoft NTFS file system.
- Flash drives must be encrypted with Microsoft BitLocker. Note: Only computers that run the Windows Professional version can encrypt a flash drive with BitLocker.
- Only one flash drive will be allowed per inmate. If new discovery is produced that will exceed the capacity of the existing flash drive, counsel must move the original AND the new discovery to a larger capacity flash drive.

Figure 1

Electronic Discovery at the Butler County Prison

In cases where the size of the discovery will exceed one terabyte, an attorney may provide the discovery on a USB external hard drive INSTEAD of a flash drive. Acceptable external hard drives must meet the following requirements:

- Only external hard drives that can connect to a USB Type A port will be permitted into the prison.
- External hard drives must be formatted with the Microsoft NTFS file system.
- External hard drives must be encrypted with Microsoft BitLocker.
- Only one external hard drive will be allowed per inmate.

Protective Orders

If the discovery is covered by a protective order, the attorney must provide a copy of the order with the discovery media.

Media Preparation Process

The process for preparing a flash drive or external hard drive requires a computer running Windows Professional version 10 or higher. The steps are as follows:

1. *FORMAT THE MEDIA WITH THE NTFS FILE SYSTEM*
   - Insert the media into an available USB port on the computer and determine which drive letter has been assigned to the disk.

   - Open the Windows File Explorer.

   - Right-click on the flash drive and select "Format".
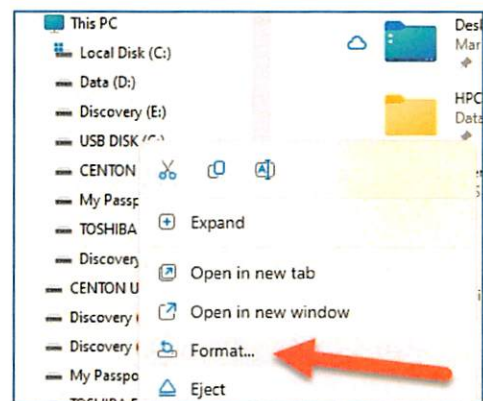
Electronic Discovery at the Butler County Prison

- When the dialog box appears, change the File System to "NTFS", and change the volume name to the pattern:

  LastName-FirstInitial

- In the screenshot on the right, the name is "**Jackson-V**".

- Click "Start" and wait for the formatting to complete.

- When the process is finished, click "OK", and then "Close".
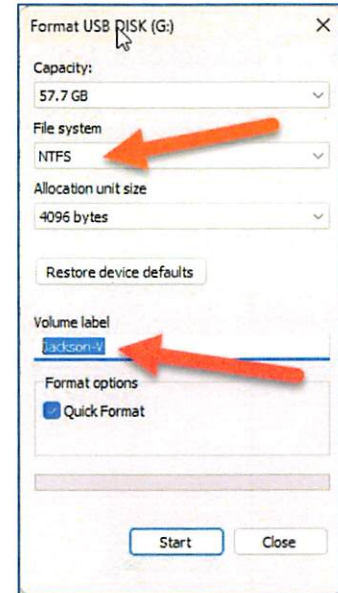
2. ENCRYPT THE MEDIA WITH WINDOWS BITLOCKER

- In the search box next to **Start** on the Task Bar, type "bitlocker" (See arrow at the bottom of the screenshot).

- The item named "Manage BitLocker" will appear at the top of the search menu".
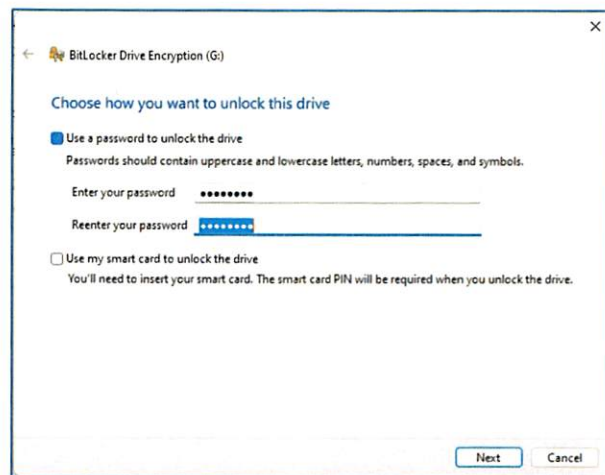
- Click on "Manage BitLocker".
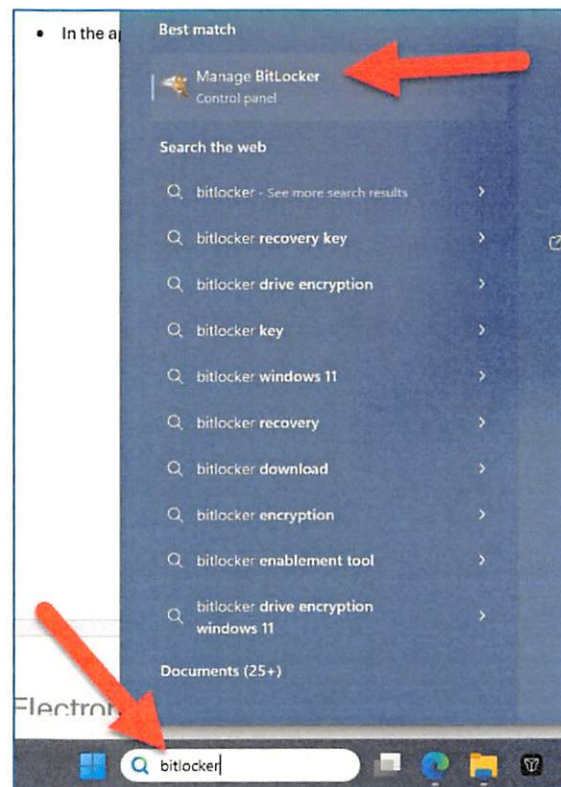
Electronic Discovery at the Butler County Prison

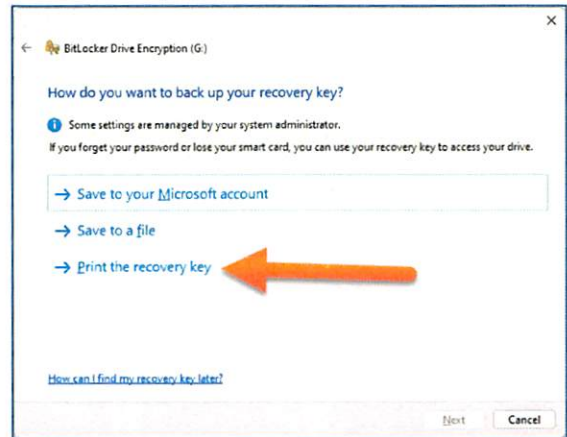- Locate the drive you just formatted in the list under "Removable data drives – BitLocker To Go".
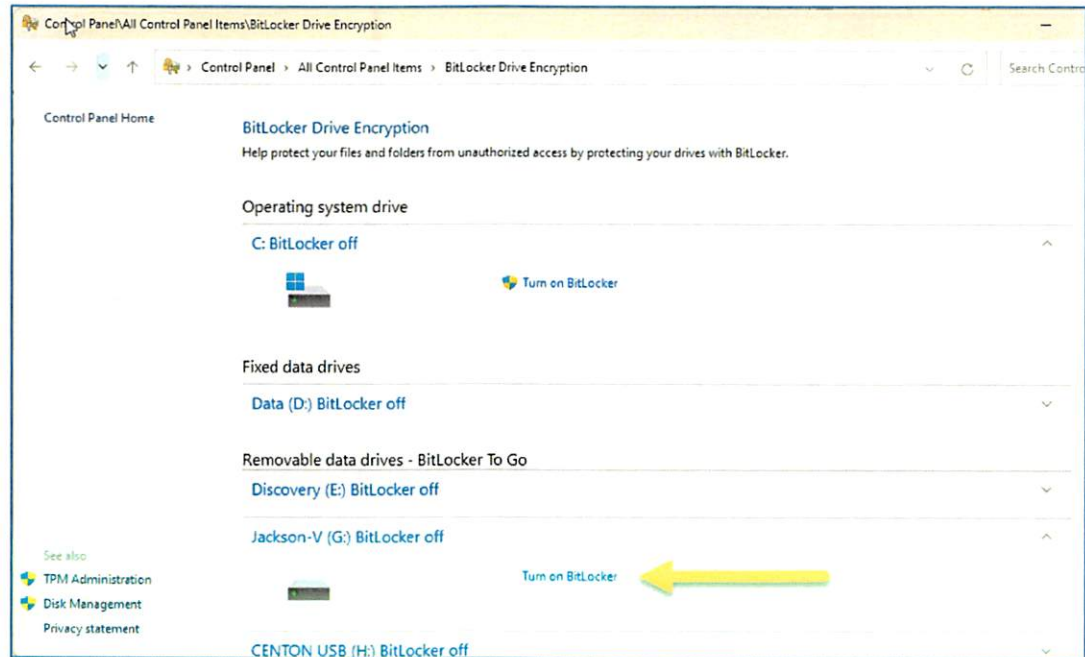
- Click "Turn on BitLocker".

- Enter your preferred password in the dialog box. Fill in both boxes.
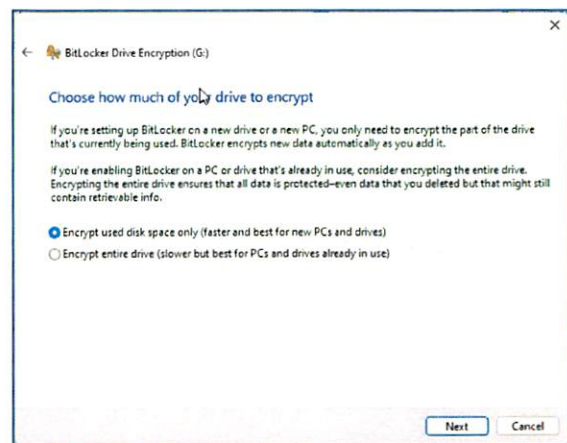
- Click "Next".

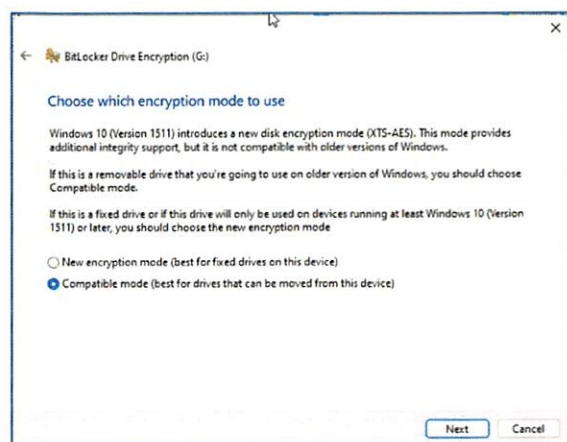# Electronic Discovery at the Butler County Prison

- For the recovery key, select "Print the recovery key".

- When the key has successfully printed, click "Next".

- The next screen will ask you how much of the drive to encrypt.

- Select "Encrypt used disk space only (faster and bet for new PDs and drives)."
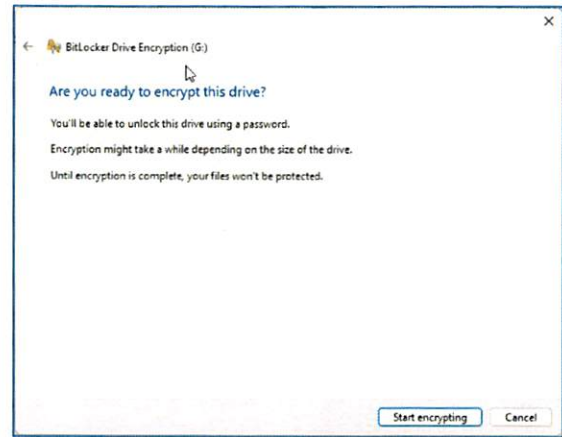
- Click "Next".

- The next screen will ask you which encryption method to use.

- Select "Compatible mode (best for drives that can be moved from this device)".
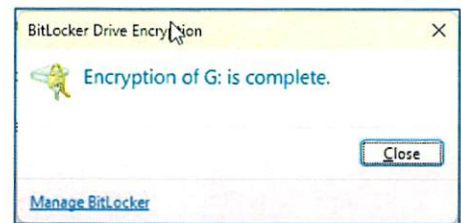
- Click "Next".

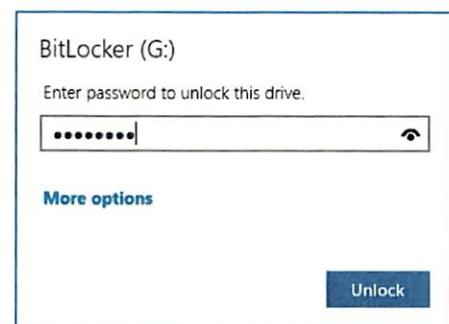# Electronic Discovery at the Butler County Prison

- The final screen will ask you whether you are ready to encrypt the drive.

- Select "Start encrypting".

- When the encryption process is complete, the dialog box on the right will appear.

- Select "Close".

- Once the process is complete, test the encryption by safely removing the drive, and then reinserting it.

- When the dialog box appears, enter your password.

- If your password works, the drive should appear with the correct volume name in the File Explorer.

Electronic Discovery at the Butler County Prison

Completing the Task

- Copy the discovery to the encrypted flash drive.

- Test each type of discovery to make sure it works.

- While testing the discovery, take screenshots and/or create instructions for the client to use.
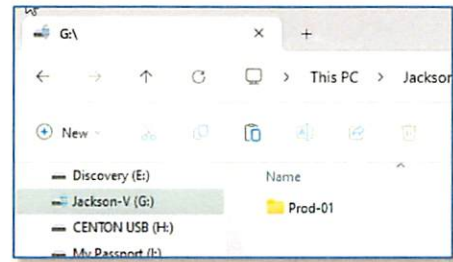
Submitting the Flash Drive

- When the flash drive ready for the client, mail the drive and the instructions to:

  Commonwealth eDiscovery, LLC
  194 West Steuben Street
  Pittsburgh, PA 15205

- The staff at Commonwealth eDiscovery will write-protect the flash drives and deliver them to the prison. There is no cost associated with this process.

- If you would prefer to delegate the task of preparing the flash drive and processing the discovery files, Commonwealth eDiscovery is able to provide that service for an additional fee.

- Contact Commonwealth eDiscovery at (412) 339-0076 or cases@cwediscovery.net for more details.