**[COMPANY NAME]**

**EMPLOYER TURNOVER**

**WORKSTATION LITIGATION HOLD**

**Standard Operating Procedure**

**Manual**

**DATE:**

**VERSION:**

**SECTION 1: Creation of Legal Hold External USB Drive to Hold Forensic Images**

**A. Preparation of the “Target” Drive to hold the forensic image**

Before beginning the forensic imaging process, please prepare a Bitlocker encrypted external USB drive which will be used to hold the forensic image; this external USB drive will be known as the “Target” drive, to which the forensic image of a workstation’s internal hard drive will be written.

1. Applying BitLocker Encryption to the Target drive
2. Once the Target drive is plugged into your workstation, open Windows Explorer and navigate to the Target drive.
3. Right mouse click on the Target drive, and then left mouse click on “Turn on BitLocker”.
4. When the below BitLocker menu opens, check the box “Use a password to unlock the drive”
5. Enter the same password into the “Enter your password” and “Reenter your password” boxes”.
6. A good password naming convention is **YYYYMMDD\_[COMPANY NAME]**; for example **20181119\_[COMPANY NAME]**
7. Once you have entered and reentered the password, left mouse click on “Next”



1. Save the BitLocker Recovery Key to a file by choosing “Save to a File”



1. Save the Bitlocker Recovery Key file to a folder named “BITLOCKER RECOVERY KEY” on your computer desktop. This BitLocker Recovery Key file will be required to unlock the Target drive in the event the BitLocker password is forgotten.



1. Select “Encrypt used disk space only (faster and best for new PCs and drives)



1. Choose “Compatible mode (best for drives that can be moved from this device) and left mouse click on “Next”.



1. Left mouse click on “Start encrypting”



The BitLocker encryption process should take less than one minute to complete. Once encryption is complete, the following message will appear:



When looking at the “Target” drive in Windows Explorer, one will now see a silver padlock next to the drive indicating the drive has been successfully BitLocker encrypted:

 

**SECTION 2: Creation of the Forensic Image**

In order to create a forensic image of employee workstations, we will be using AccessData’s FTK Imager Forensic Imaging tool. FTK Imager is a forensic imaging tool commonly used by U.S. and international law enforcement professionals.

FTK Imager may be downloaded from the following location:

* **FTK Imager Lite version 3.1.1**

DOWNLOAD LINK: https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1

After you have downloaded FTK Imager Lite Version 3.1.1, please copy the entire software folder to the Target drive so that the folder holding the FTK Imager Lite software is at the root of the Target drive. :



****

1. Once you have launched FTK Imager Lite, please left click on the “File” choice at the top left of the screen, which will bring up a drop down menu with the the below options. Please left click on the option “Create Disk Image….”

****

1. When the next menu pops up, left click on the fourth choice from the top, “Logical Drive”.



1. In the “Source Drive Selection” drop down menu, please select “**C:\ - [NTFS]**” and then left mouse click on the “Finish” button



1. In the “**Create Image**” menu, please make sure that the “**Verify images after they are created**”, “**Precalculate progress statistics**” and “**Create directory listings of all files in the image after they are created**” boxes are checked. Then, please left mouse click on the “**Add…**” button.



1. In the “**Select Image Type**” menu, please select the “**E01**” option seen below. Then please left mouse click on the “**Next>**” button.



1. In the “**Evidence Item Information**” menu, please enter the following information:
	1. **“Case Number:”** Please enter a Case Number, if available, which will be provided by [COMPANY NAME] Counsel. If there is no case or related law suit, please enter the same information found in the below “**Evidence Number:**” field in the “**Case Number:**” field.
	2. **“Evidence Number:”** Please enter a unique number based upon the type of device being imaged. For example, the first laptop of five laptops being imaged for a specific matter would be “**PUSL42125-JDOE”**. NOTE: “**PUSL42125”** is [COMPANY NAME]’s internal workstation tracking number and **“JDOE”** is the first initial and last name of the employee to whom the workstation was assigned.
	3. **“Unique Description:”** Please enter the workstation **Make**, **Model** and **Serial Number** here of the workstation being forensically imaged.
	4. **“Examiner:”** Please enter your first and last name here.

Then, please left mouse click on the **“Next>”** button.



1. On the “**Select Image Destination**” menu, please left click on “**Browse**” at the top of the “Select Image Destination” tab in order to select the folder location that the forensic image file will be saved to.



1. Please select the BitLocker encrypted drive, in the below example “**[COMPANY NAME] (G:)**”. Please left mouse click on the “**Make New Folder**” button and create a new folder to hold the forensic image file. In the below example, the forensic image file will be created, or saved to the “**PUSL42125-JDOE”** folder.

 

1. In the “**Select Image Destination**” menu, in the “**Image Filename (Excluding Extension)**” box second row down from the top, type in the [COMPANY NAME] workstation tracking number “dash” the first initial and last name of the employee who used the workstation. In the below example we see “**PUSL42125-JDOE**”. This will allow for easy identification of the forensic image.

Please change the “**Image Fragmentation size (MB)**” value to “**0**”.

Please change the “**Compression**” value to “**9**”.

Please do not check the box called “**Use AD Encryption**”.

Please left mouse click on the “**Finish**” button.



1. In the “**Create Image**” menu, please left mouse click on the “**Start**” button to begin the forensic imaging process. In the screenshot below, one can see that a forensic image file named “PUSL42125-JDOE.E01” will be created on the “G:\” drive in a folder named “**PUSL42125-JDOE**”.



1. Once the forensic image has been successfully created, a window will appear called “**Drive/Image Verify Results**” as seen in the example below.

If the “**Verify result**” value equals “**Match**”, then a successful bit-for-bit forensic image has been created of the workstation internal hard drive.

All FTK Imager open windows may be closed at this point as the forensic imaging process is successful and complete!



* “**MD5 Hash**” – This is a unique value calculated using a standard mathematical algorithm and is a court accepted method of determining if a file is a true forensic copy of another file.
* “**SHA1 Hash**” – This is another more complex unique value calculated using a standard mathematical algorithm and is a court accepted method of determining if a file is a true forensic copy of another file.