TEXAS HHSC WIC PROGRAM
Certification of Data Sanitization

The State Agency requires that all devices, prior to all forms of disposal, be completely sanitized of all data to remove all confidential information (Policy AC:07.0).

Complete this form for all computers, mobile phones and associated equipment with electronic storage being disposed of by a WIC Local Agency and keep it on file.

	Asset Tag	Serial Number	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

I hereby certify that the above listed assets have had all data removed from them.

_____	_____	_____
WIC Director	Signature	Date
_____	_____	_____
IT Dept. Rep.	Signature	Date

WIC Instructions for Data Sanitization

The object of sanitization is to leave the data on a storage device in an unreadable condition prior to disposal. How this is achieved depends on the specific type of device and its storage medium.

There are two basic processes that are used.

1. Overwriting data multiple times with different patterns
2. Encrypting the storage device

Both methods may be used for convention magnetic hard disk drives (HDD), whether internal or external (USB). Encryption is the only method recommended for memory-based storage devices (e.g. SD cards, flash drives, solid-state drives).

If unsure of the type of storage, use system information options or applications to find the information.

How to Sanitize Magnetic HDDs with DBAN

1. Download the DBAN software .ISO file.
   https://sourceforge.net/projects/dban/
2. Download the RUFUS application and use it to make a bootable DBAN USB drive.
   https://rufus.ie/
3. Follow the directions below to create the bootable USB drive and then use it to sanitize the drive.
   https://dellwindowsreinstallationguide.com/cleaning-up-a-drive-format-vs-secure-wipe-ssd-and-hdd/securely-wipe-your-hard-drive-with-dariks-boot-and-nuke-dban/

How to Sanitize HDDs and Memory-Based Storage Devices

1. For Windows 7/8/10 Professional, use BitLocker.
   - After encrypting the device, remove the encryption key.
   - Open a Command Prompt (admin rights) and type: Manage-bde -forcerecovery c:
   - Without doing anything else, shut the computer down.
2. For Macintosh OS X Lion or later, use FileVault 2.
   - After encrypting the device, remove the encryption key.
   - Restart the computer.
   - Hold down the Command+R keys when the grey startup screen appears.
   - Select the Disk Utility.
   - Highlight the drive and select the Erase tab.
   - Erase the drive, accepting the default settings.

3. The open-source encryption software, VeraCrypt, may also be used. It's available for Windows, Mac OSX, and Linux.
   https://www.veracrypt.fr/en/Downloads.html

   https://askleo.com/how-do-i-encrypt-a-hard-drive-using-veracrypt/

   - Use a very long random password that cannot be remembered by anyone.

How to Sanitize Smartphones and Tablets

1. Research the encryption settings for the operating system version installed on your device.
2. Enable encryption and encrypt the device's onboard storage. Ensure that the process completes successfully.
3. Reset the device to factory settings.

How to Sanitize Standalone Flash Devices (SD cards, USB drives)

1. Insert the device into a computer.
2. Download the latest portable version of VeraCrypt compatible with the operating system
   (Windows, OSX) running on the computer.
   https://www.veracrypt.fr/en/Home.html
3. Use VeraCrypt to encrypt the entire memory device.
4. See the section Using VeraCrypt.
   https://askleo.com/how-do-i-encrypt-a-hard-drive-using-veracrypt/
   - Use a very long random password that cannot be remembered by anyone.