SANITIZATION AND DISPOSAL OF ELECTRONIC DEVICES

OCTOBER 2020

ITSAP.40.006

Many of the electronic devices we use today store personal or sensitive information. When our devices (e.g. tablets, smartphones, or computers) become surplus to our needs, we look for ways to dispose of them (e.g. donate, recycle, or resell). However, your unwanted equipment may still contain personal or sensitive information. Before you get rid of devices (e.g. your external hard drive, camera, or gaming console) you should sanitize the device and any associated media. For work devices, or personal devices that you use for work, check your organization's information management policies to ensure business information is handled appropriately, such as saved to a corporate repository.

WHAT IS DEVICE SANITIZATION?

Sanitization is the process of permanently removing data from a device or storage media. The storage media can be reused, but the data cannot be recovered or accessed.

IS DELETING THE SAME AS SANITIZATION?

In short, no. Data is still recoverable when deleted or moved to the trash or recycle bin. Sanitization is a more involved process. When you take the time to properly sanitize your unwanted electronic devices, you are ensuring that all data is removed from your device and preventing the unintentional disclosure of personal or sensitive information.

Don't forget about backups.

Before sanitizing or erasing any device, consider backing it up, just in case you delete something by mistake.

HOW CAN I SANITIZE MY ELECTRONIC DEVICES?

The Cyber Centre recognizes four main methods of sanitization:

1. **Erase and factory reset:** This method is available on many devices. When reset, the data is no longer accessible through the device's user interface. However, when a device is reset, the data is not truly erased. Data on external media, such as memory and SIM cards, are not erased by the factory reset command and must be disposed of separately.

2. **Overwrite and secure erase (SE):** This method sanitizes all types of media, including magnetic storage media like hard drives, for reuse or disposal. However, overwrite and SE is damaging, and it shortens the life of solid state flash media, which may interfere with reuse.

This method uses software to write multiple passes (3 or more series) of random binary code (zeros and ones) on the storage media to prevent anyone from reading the previous data. If the media contains highly sensitive data, use overwrite and SE with physical destruction.

3. **Crypto erase (CE):** This method securely deletes the encryption key used to encrypt data on the media. The encrypted data remains on the media, but it is unreadable and unrecoverable because the key has been removed. CE is suitable for encrypted hard drives, solid-state drives, and other flash-based storage devices if encryption has been used from the beginning of the media's life cycle.

4. **Degaussing:** Degaussing uses a magnetic force to erase all stored data elements on a magnetic tape, a hard drive, a floppy disc, or a magnetic stripe card. Solid-state devices (including all flash-based devices like USB keys) cannot be erased using degaussing.

If you are unsure about how to carry out any of the methods mentioned above, you should consult the device manufacturer's website, owner's manual, or your service provider for information on how to permanently delete your personal information.

Don't forget about disconnecting your unwanted devices from your online accounts.

Examples of devices that you should sanitize before disposing of them:

- PCs (internal hard drives)
- Routers
- CDs and DVDs
- Smartphones
- Memory cards
- Tablets
- E-readers
- Digital cameras
- Media players
- Printers
- Smart monitors
- Storage media
- Video game consoles
- Smart watches
- Smart TVs

WHAT ABOUT PHYSICAL DESTRUCTION OF THE DEVICE?

In some cases, physical destruction of the device or media (along with proper sanitization) is the best option to ensure sensitive data is made inaccessible.

Common methods of secure destruction include:

- Crushing
- Shredding
- Disintegration

Many office shredders can shred CDs and DVDs. You can use tools like a hammer or a drill to do the job (be sure to wear safety equipment), but this is usually only effective in making equipment non-functional. Instead, we suggest taking your item to a trusted destruction facility. Destruction should be considered if you have highly sensitive data on your device.

HOW CAN I DISPOSE OF UNWANTED ELECTRONIC DEVICES AND MEDIA (E-WASTE)?

Once you are confident that your device no longer contains sensitive information, and you are not planning on repurposing, selling, or donating the device to someone else, you can safely dispose of the e-waste.

Donating your electronics for reuse or recycling helps keep e-waste from piling up in landfills. Recycling also allows some resources found in the devices (e.g. recyclable plastics and gold) to be recovered.

You can find an inventory of recycling programs on the Environment and Climate Change Canada website. The inventory provides links to extended producer responsibility programs, product stewardship programs, and other programs that accept e-waste.

LEARN MORE

For more detailed information on sanitization, see our publication, *ITSP.40.006 IT Media Sanitization*, which is available on the Cyber Centre website (**cyber.gc.ca**).

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**