Data Destruction

Data destruction is removing or destroying data stored on electronic devices so that an operating system or application cannot read it. Data destruction is required when a company no longer needs a device, when there are unused or multiple copies of data, or you are required to destroy specific data.

There are three categories of data destruction methods: recycling, physical destruction, and third-party destruction. This reading will introduce the data destruction methods and how to decide which method to use.

Recycling

Recycling includes methods that allow for device reuse after data destruction. This option is recommended if you hope to reuse devices internally, sell surplus equipment, or your devices are on loan and are due to be returned. Standard recycling methods include the following:

- **Erasing/wiping**: cleans all data off a device's hard drive by overwriting it. Erasing or wiping data can be done manually or with data-destruction software. This method is practical when you only have a few devices that need data destroyed, as it takes a long time. Note that it may take multiple passes to wipe highly sensitive data completely.
- **Low-level formatting:** erases all data written on the hard drive by replacing it with zeros. Low-level reformatting can be done using a tool such as HDDGURU on a PC or the Disk Utility function on a Mac.
- **Standard formatting:** erases the path to the data and not the data itself. Both PCs and Macs have internal tools that can perform a standard format, Disk Management on a PC or Disk Utility on a Mac. Note that standard formatting does not remove the data from the device, enabling data rediscovery using software.

Physical destruction

Physical destruction includes any method that physically destroys a device to make it difficult to retrieve data from it. You should only use physical destruction if you do not need to reuse the device. However, only completely destroying the device ensures the destruction of all data with physical methods. Physical destruction methods include the following:

- **Drilling** holes directly into the device wipes data out on the sections where there are holes. However, individuals can recover data from the areas that are still intact.
- **Shredding** includes the physical shredding of hard drives, memory cards, CDs, DVDs, and other electronic storage devices. Shredding reduces the potential for recovery. Shredding requires special equipment or outsourcing to another facility.
- **Degaussing** uses a high-powered magnet which destroys the data on the device. This method effectively destroys large data storage devices and renders the hard drive unusable. As electronic technology changes, this method may become obsolete
- **Incinerating** destroys data by burning the device. Most companies do not have an incinerator on-site. Devices need to be transported to a facility for incineration. Due to this, devices can be lost or stolen in transit.

In addition to effectively destroying data on electronic devices, it is essential to follow best practices for electronic device disposal.

Outsourcing

Outsourcing means using a third-party specializing in data destruction to complete the physical or recycling process. This option appeals to companies that do not have the staff or knowledge to complete the destruction themselves. Once a vendor has completed the task, they issue a certificate of destruction/recycling.

The certificate of destruction serves as a statement of completed destruction of data on electronics, hard drives, or other devices. The certificate includes the client's contact information, date of service, vendor company name, manifest, signature, method of destruction, and legal statement. However, exercise caution as the certificate does not indicate a level of training, auditing, or any other verification that a vendor is knowledgeable about data destruction.

Key Takeaways

Data destruction makes data unreadable to an operating system or application. You should destroy data on devices no longer used by a company, unused or duplicated copies of data, or data that's required to destroy. Data destruction methods include:

- **Recycling:** erasing the data from a device for reuse
- **Physical destruction**: destroying the device itself to prevent access to data
- **Outsourcing**: using an external company specializing in data destruction to handle the process

Resource for further information

For more information about disposing of electronics, please visit Proper Disposal of Electronic Devices, a resource from CISA.

Mark as completed

Like **Dislike** **Report an issue**