ARTICLE

Data sanitisation enables more sustainable data centre ITAD

IRON MOUNTAIN®
ASSET LIFECYCLE MANAGEMENT

With the e-waste problem growing in scope and severity, data centre managers need to broadly adopt sustainable practices to comply with corporate social responsibility initiatives and increasing environmental regulations. Data sanitisation should be a core practice.

Sustainable IT asset disposition (ITAD) aims to minimise the environmental impact of disposing of IT equipment. When data centre equipment reaches end of use, data sanitisation ensures that sensitive information is securely removed before repurposing, reselling or disposal via recycling. This process not only reduces the risk of data breaches but also lessens the need for additional asset manufacturing, thus conserving resources and minimising electronic waste.

Data sanitisation is the deliberate, permanent removal of data from IT assets to prevent unauthorised access to sensitive information after asset retirement. These steps ensure that sensitive information like financial records, personally identifiable information, or intellectual property doesn't fall into the wrong hands.

What is data sanitisation?

A device is considered sanitised when it has no recoverable data, even with advanced forensic tools. According to the International Data Sanitisation Consortium, there are three ways to sanitise storage and memory devices.

Data erasure uses software to overwrite all data with zeros and ones securely. While considered effective, it is a time-consuming process and doesn't work on solid-state drives (SSDs) and certain types of flash storage.

Cryptographic erasure is another software-based technique that encrypts the entire device and then erases the decryption key, rendering the data impossible to access. It's most effective when used with a minimum of 128-bit encryption. Careful key handling is critical. Failing to destroy the key when erasure is complete can leave data vulnerable. Some regulatory frameworks and legal requirements also don't recognise cryptographic erasure as a valid form of data sanitisation.

Physical destruction takes two forms – degaussing and shredding

- Degaussing exposes the device to a powerful magnetic field that makes the data unrecoverable. It's an effective and environmentally friendly data erasure technique that works quickly and enables drives to be reused. The downside is cost. Industrial-grade degaussers can run to more than $10,000. Using a degaussing service is more cost-effective in most cases.
- Disk drive shredding disintegrates storage devices into unrecoverable pieces. It's considered the most effective form of data sanitisation, but it is also the least environmentally friendly since shredded assets can't be reused or resold and shredded materials can only be recycled, thus incurring additional costs. While shredding is the only option when drives are irreparable or can't be erased with software, physical destruction can release hazardous chemicals unless the work is done by a vendor certified in Responsible Use and Recycling (R2) practices.

All three methods are appropriate for use with hard disk drives. Solid state drives (SSD) must be erased with software built into most models' firmware or with specialised third-party tools. Memory devices should be wiped clean using specialised software that passes Test Level 2 of the Asset Disposal and Information Security Alliance Threat Matrix.

Data centre managers should also be aware of data erasure methods that are not considered sufficient to qualify as sanitisation.

- Data deletion merely hides data until it's overwritten, leaving it recoverable.
- Reformatting a disk doesn't fully erase its contents; data is usually recoverable using forensic tools.
- Factory resets on devices like mobile phones and tablets remove user data and restore factory settings, but effectiveness varies by manufacturer.
- Uncertified data wiping and file shredding don't follow specific standards or provide formal proof of sanitisation.

Documented destruction

Regardless of the method you use, sanitisation should be documented. Analysts advise using an ITAD vendor that "provides a certificate of data destruction with a serialised inventory of the data-bearing assets sanitised." The vendor should give you the right to audit its data sanitisation processes and standards to ensure compliance with your needs.

The most sustainable and environmentally responsible data sanitisation techniques are those that allow for the safe reuse of IT assets. Devices such as servers, hard drives, and SSDs can be repurposed or resold, extending their life cycle and reducing the need to manufacture new products. This circular approach both conserves resources and cuts down on e-waste.

In short, data sanitisation is a win-win: It enhances data security while advancing a more sustainable IT lifecycle and can even yield revenue from resale. In some jurisdictions, it's also the law.