

# Data sanitization enables more sustainable data center ITAD

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

Sustainable IT asset disposition (ITAD) aims to minimize the environmental impact of disposing of IT equipment. When data center equipment reaches end of use, data sanitization 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 minimizing electronic waste.

Data sanitization is the deliberate, permanent removal of data from IT assets to prevent unauthorized 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 sanitization?

A device is considered sanitized when it has no recoverable data, even with advanced forensic tools. According to the [International Data Sanitization Consortium](#), there are three ways to sanitize 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 recognize cryptographic erasure as a valid form of data sanitization.



**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 sanitization, 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 specialized third-party tools. Memory devices should be wiped clean using specialized software that passes Test Level 2 of the [Asset Disposal and Information Security Alliance](#) Threat Matrix.

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

- 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 sanitization.

## Documented destruction

Regardless of the method you use, sanitization should be documented. [Analysts advise](#) using an ITAD vendor that "provides a certificate of data destruction with a serialized inventory of the data-bearing assets sanitized." The vendor should give you the right to audit its data sanitization processes and standards to ensure compliance with your needs.

The most sustainable and environmentally responsible data sanitization 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 sanitization 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.

---

## ABOUT IRON MOUNTAIN

For over 70 years, Iron Mountain Incorporated (NYSE: IRM) has been your strategic partner to care for your valuable assets. A global leader in storage and information management services, and trusted by more than 225,000 organizations around the world, including 95% of the Fortune 1000, we protect, unlock, and extend the value of your information and assets—whatever they are, wherever they are, however they're stored. We provide the framework necessary to bridge the gap between physical and digital and extract value along the lifecycle of your information, enabling organizational resilience. And all this with a commitment to sustainability at our core.

© 2024 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated in the U.S. and other countries. All other trademarks and registered trademarks are the property of their respective owners.

