IRON MOUNTAIN®

ASSET LIFECYCLE MANAGEMENT

Minimise Data Risk, Maximise Critical Business Outcomes

Hyperscale-grade audit compliance.

Iron Mountain's comprehensive approach to data security compliance provides complete traceability and peace of mind. Here's how it works:

STEP 1

Assets discovered

The first step in establishing a robust audit trail for asset decommissioning is asset discovery, which occurs when we compare your asset list with the results of our discovery process. Our proprietary data sanitisation and compliance software, Teraware™, automates the discovery of every serialised asset and maintains parent-child data relationships to ensure precise auditing and tracking. More specifically, Teraware identifies server components (e.g., CPU, Memory DIMMs) and key drive attributes (e.g., power-on hours, logical serial number). This information provides a detailed blueprint of the relationships between the rack, server, and drive.

Teraware's automated reconciliation reporting is critical to establishing accurate inventory and ensuring complete sanitisation.

STEP 2

First reconciliation report generated

Upon completion of asset discovery, we run an automated reconciliation that generates a variance analysis. This analysis serves to:

- Identify variances between discovered assets and your inventory
- Ensure all variances are researched and resolved before advancing in the decommissioning process

By meticulously addressing discrepancies, we maintain transparency and compliance throughout the asset lifecycle management process.

STEP 3

Drives erased

After the first reconciliation, Teraware securely and comprehensively removes all data from functional data storage devices, ensuring data protection and policy compliance. The erasure process involves:

- Setting up a dedicated virtual local area network (VLAN)
- Connecting a Teraware appliance to the assets to be decommissioned via the dedicated VLAN
- Automatically sending agents to every server node in the set of target assets
- Instructing agents to automatically erase data
- Providing job status reporting throughout the process

On average, Teraware successfully erases 95-98% of drives, but typically a small number of drives will fail. For the devices that fail automated erasure, we follow the National Institute of Standards and Technology (NIST) and the National Association for Information Destruction (NAID) guidelines for secure and efficient physical destruction. Leveraging the detailed blueprint created during asset discovery, we can quickly locate and pull the failed devices, then physically scan and mark them for destruction. Physical destruction of data-bearing devices can be completed either on-site, using a mobile shredding unit, or by securely shipping them to an Iron Mountain facility for destruction.

STEP 4

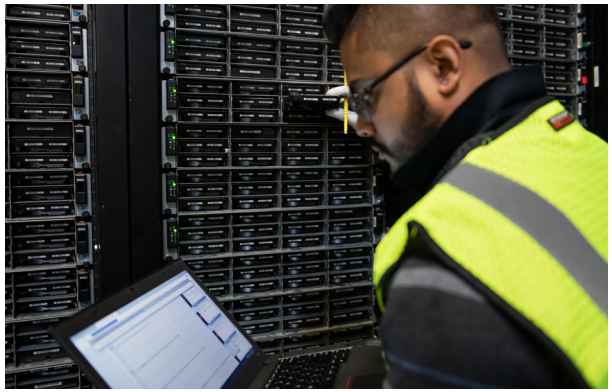
Certificates created

Upon completion of the erasure process, we automatically generate a Certificate of Sanitisation for each successfully sanitised drive. For drives that fail the erasure process and undergo physical destruction, we issue Certificates of Destruction.

These certificates serve as essential evidence of complete data elimination, ensuring audit compliance and security throughout the asset lifecycle management process.

No data has ever been discovered on a device wiped with Teraware.*

*According to multiple tests conducted by independent forensic labs.



STEP 5

Departure report generated

After the erasure process, we generate a departure report to account for all processed assets and their designated destinations. The creation of the departure report involves:

- Creating an asset reconciliation report that identifies and categorises the processed assets
- Designating assets to be shipped to an Iron Mountain facility
- Cross-checking Teraware's automated report with physical scans of items

The departure report serves as an additional layer of security and guarantees accurate asset tracking, whether assets are shredded at the data centre, or shipped to Iron Mountain for remarketing or destruction. This systematic approach, with careful attention to detail, reinforces audit compliance and security throughout the decommissioning process.

STEP 6

Assets securely transported

Iron Mountain ensures secure transportation of your decommissioned assets to our processing facilities. As the equipment is loaded onto securely sealed trucks, we cross-check each item against the Teraware report for accurate asset tracking.

Our secure shipping measures, including sealed loads and GPS tracking, allow you to monitor your assets' location throughout the transportation process.

STEP 7

Final reconciliation completed

At the Iron Mountain facility, we perform another thorough reconciliation to ensure that all assets were successfully received. This reconciliation process involves:

- Cross-checking assets against the baseline report upon arrival and unloading
- Scanning items individually into our web portal
- Cross-checking the web portal's data with Teraware to reconcile each serialised asset independently

If we identify discrepancies, we generate a variance report and initiate an investigation in collaboration with the client to resolve the issue.

STEP 8

Maximum value recovered

Iron Mountain maximises value recovery for resalable assets while maintaining security and client anonymity. The preparation process for resale includes:

- Removing asset tags to ensure security and prevent misidentification
- Reconditioning assets and components for performance and cosmetic upgrades
- Securely packaging hardware for a retail-grade final product
- Resetting firmware to factory settings for client protection

Upon selling the assets, Iron Mountain notifies the client, distributes resale funds, and completes the chain of custody. Our web portal offers complete tracking throughout the process, ensuring transparency and peace of mind for our clients in the asset lifecycle management process.

Non-remarketed assets destroyed & recycled

Iron Mountain assures secure and environmentally responsible asset destruction and recycling. Before disassembly and recycling, we remove asset tags from racks and servers to maintain client data security and prevent future misidentification of equipment.

Failed drives are securely shredded, and we create a Certificate of Destruction for each drive as proof of proper disposal. Clients can also choose to have fully sanitised drives shredded for additional security if desired.

Mission citical visibility
Whether you have your drives sanitised, destroyed, or both, Iron Mountain's web portal makes the process fully transparent and closes the loop on your data security.

Peace of Mind. Guaranteed.

From erasing and shredding drives to recycling or reselling racks, servers, and other equipment, Iron Mountain maintains a fully traceable audit trail – ensuring end-to-end compliance. We stand by our results: thanks to our complete chain of custody, our clients have all received flawless results on audits by top-tier, independent auditors.

Trust your critical corporate and data centre IT assets to the experts. **Trust Iron Mountain.**

IRON MOUNTAIN®

1300 476 668
IRONMOUNTAIN.COM/AU
0800 732 255
IRONMOUNTAIN.COM/NZ

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 organisations 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 organisational resilience. And all this with a commitment to sustainability at our core.