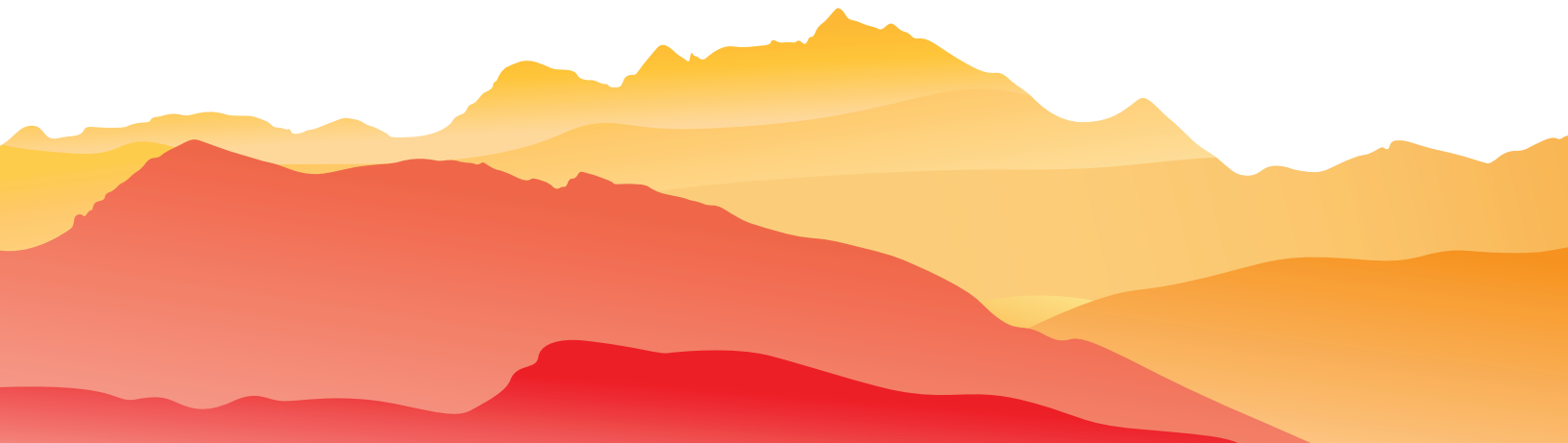
IRON MOUNTAIN®

ASSET LIFECYCLE MANAGEMENT

White paper

Teraware

Secure, scalable data sanitization engineered for the data center, exclusively from Iron Mountain



Contents

Introduction

When people hear "data erasure" or "data wiping", it often suggests a generic process for removing data from storage.

With years of experience processing millions of storage devices annually, Iron Mountain understands that simple overwriting is insufficient. Meeting rigorous business sanitization standards is essential to safeguard against data breaches and data theft, addressing the high-stakes requirements of security-conscious organizations worldwide.

Teraware, designed specifically for enterprise needs, is a secure and highly effective data sanitization platform. Developed and refined over more than a decade, Iron Mountain continues to evolve Teraware to meet the demands of the world's most advanced and sophisticated data centers.

Teraware ensures complete data erasure for functional devices while flagging non-functional drives that cannot be sanitized. It provides a fully traceable audit trail and certification process, meeting the high standards expected by industry leaders worldwide and aligning with best-practice demands for secure, thorough data management.

Engineered specifically for data center environments, Teraware excels in technologically complex IT settings and simplifies intricate processes. It securely sanitizes mainstream storage types, both onsite and remotely, with scalability for large projects. When hardware errors prevent successful sanitization, Teraware quickly flags those devices for secure destruction.

This paper will review the processes and specific steps associated with a comprehensive data sanitization process across storage media types– including detailed drive discovery, asset specification mapping, handling failed or non-conforming assets and issuing Certificates of Sanitization. We will also explore how Teraware scales smoothly to handle decommissioning at the hyperscale and enterprise data center level performing these large-scale operations safely, securely and at speed.

A brief history of Teraware

In 2007, ITRenew, now part of Iron Mountain, saw increasing customer demand for data sanitization of hard disk drives to enable remarketing of successfully sanitized media. The available options on the market had fundamental limitations such as:

Scaling: High-volume media sanitization lacked the ease and efficiency required to handle it effectively at scale

Reporting: Reports lacked the customization needed to align with specific auditing protocols

Security: Protocols struggled to keep up with evolving industry standards

Scaling

Media could not be sanitized with ease and efficiency at high volume.

Reporting

Customization of reports for specific auditing protocols was lacking.

Security

Protocols barely kept pace with evolving industry standards.

Additionally, these solutions were slow to support new device types—if they added support at all.

We set out to create a superior solution that addressed the gaps in scalability, functionality, and support present in existing commercial tools. The first version of Terawipe, launched in 2008, was designed for use in our processing facilities, enabling high-volume data sanitization of drives.

After launching Terawipe, we identified an industry need for in-rack data sanitization, which offers faster, more secure, and cost-effective solutions compared to manually removing drives for erasure. We collaborated with top hyperscalers' InfoSec teams to address their primary concerns: data security, audit trails, and detailed sanitization certifications.

Building on our work with hyperscalers, we expanded the solution from an internal tool into a robust platform, applying rigorous development methodologies that culminated in the creation of Teraware.

Introduced in 2014, Teraware became our second-generation digital asset disposition platform. Building on Terawipe, the new agent engine added discovery, overwrite, and verification tasks. With additional components, its capabilities and performance expanded significantly, marking the shift from simple data erasure to a comprehensive data sanitization platform.

> The Teraware platform marked the turning point from "data erasure" to true "data sanitization."

Today, many of the largest data center operators in the world rely on Iron Mountain and our industry-leading Teraware platform for secure data center decommissioning. Over 10 million drives have been sanitized with Teraware since its introduction, and no data has ever been recovered even with forensic tools.

Teraware overview

Teraware is a platform-based tool designed for the secure disposition of storage components from production use. It provides a fully deployable, self-contained operating environment that performs asset discovery, sanitization, and report generation.

Teraware's core components:

- **Teraware server:** Coordinates and issues tasks to the Teraware agents.
- **Teraware agent:** A unique service that performs the local sanitization process by driving the Teraware engine. The agent can run simultaneously on thousands of nodes attached to the storage that is targeted for sanitization.
- **Teraware engine:** This is contained within the agent and involves low-level vectors that "talk" to the physical devices.

To maintain the highest level of security, the Teraware server can only communicate with the agent(s) and vice versa. This deliberate isolation mechanism helps to ensure that no external entities can intercept data or interfere with the data sanitization process.

Once the Teraware agent has been deployed, the Teraware processing engine will use a job task manager to employ various techniques to destroy all data on a hard disk drive (HDD) or solid-state disk (SSD) mitigating risks of a data breach incident to the fullest extent possible. Teraware will generate a Certificate of Sanitization (CoS) for successfully sanitized and verified devices.

How Teraware components work together to provide a robust platform:

- Discovers hardware attributes automatically
- Enables operators to select the devices to sanitize via a user-friendly graphical user interface (GUI)
- Equips operators with a user interface for selecting and associating a sanitization method to the selected disks
- Offers communication protocol forget/ set functions between the Teraware server and agent modules
- Allows for the monitoring and managing of progress and results via the GUI
- Includes a reporting module for generating processing reports and Certificates of Sanitization
- Provides operators with a user interface for reviewing reports

Teraware supports a wide range of data center hardware including:

Hard disk drive (HDD)
ATA-SERIAL ATA (SATA)

- ATA-PARALLEL ATA (PATA)
- SCSI-PARALLEL SCSI (PSCSI)
- SCSI-SERIAL ATTACHED SCSI (SAS)
- SCSI-FIBRE CHANNEL (FC)

Solid state disk (SSD)
ATA-Serial ATA (SATA)

- PCI AHCI-based SSD cards
- SCSI Serial Attached SCSI (SAS)
- NVMe-based Storage
- SCSI Fibre Channel (FC)

When any of these disk types are selected, Teraware associates a sanitization standard to the disks that will process the defined overwriting and verification tasks from the first logical block address (LBA) to the maximum native LBA reported by the device. If the Teraware agent is unable to complete any of the overwrite or verification tasks, then the report will show the reason for failure. It will also flag the sanitization result for the disk as a failure with no CoS generation. Devices that fail sanitization are identified by the asset's serial number and device serial number. The operator is responsible for following the organization's chain of custody procedure for handling the failed device.

Along with determining the sanitization standards, Teraware also allows the operator to configure custom jobs with various overwrites and/or verification methods. Teraware also allows for policy driven sampling of storage devices.

Standards & compliance

Teraware is compliant with the NIST 800-88 guidelines for media sanitization regarding media types, chain of custody, methods of destruction and reporting.

To ensure that data-containing devices are completely sanitized, Teraware implements several added safeguards above and beyond NIST 800-88. This involves a multi-step overwrite process, including crypto, pseudorandom number generator (PRNG), block erase, device overwrite and a verify PRNG.

It is important to remember that these safeguards are standardized within the Teraware application and ensure the typical disk sanitization process to be verified at 100%. Iron Mountain has chosen to develop Teraware to ensure maximum data security and safety for its customers. However, Teraware customers have the ability to create specific processes within the application that allow for trade-offs between speed of sanitization and depth of verification based on their organization's unique data sanitization requirements.

'Product Claims Tested' verified by ADISA

Teraware is "Product Claims Tested" (PCT) by ADISA, an industry accreditation scheme for IT asset disposal companies. This certification verifies Teraware's ability to destroy data, rendering it unrecoverable, and provides third-party evidence of Teraware's effectiveness by an independently accredited source. Products with PCT certification can be considered more trustworthy than those without verification or those with self-certified capabilities.

Teraware supports a wide range of data sanitization standards and guidelines:

Sanitization method	Overwrites	Passes and content	COS
Australia DoD ISM 6.2.92	1-pass	PRNG + Verify PRNG	YES
Canada CSEC ITSG-06	3-pass	Zeros, Ones, PRNG + Verify PRNG	YES
Canada RCMP TSSIT OPS-II	7-pass	Zeros, Ones, Zeros, Ones, Zeros, Ones, PRNG + Verify PRNG	YES
Germany BSI VSITR	7-pass	Zeros, Ones, Zeros, Ones, Zeros, Ones, Random	NO
New Zealand NZSIT 402	1-pass	PRNG + Verify PRNG	YES
NISP DoD 5220.22-M (ECE)	7-pass	Zeros, Ones, Zeros, Ones, Zeros, Ones, PRNG + Verify PRNG	YES
NISP DoD 5220.22-M	3-pass	Zeros, Ones, PRNG + Verify PRNG	YES
NIST 800-88 (1-pass)	1-pass	Zeros + Verify Zeros	YES

Sanitization method	Overwrites	Passes and content	COS
NIST 800-88 (3-pass)	3-pass	Zeros, Ones, PRNG + Verify PRNG	YES
NSA NCSC-TG-025	3-pass	Zeros, Ones, PRNG + Verify PRNG	YES
Russia GOST R 50739-95	3-pass	Zeros, Random, Random	NO
Teraware Optimized Sanitization	1-pass	Zeros or FW Assist + Verify PRNG	YES
Teraware SAS/SATA SSD Sanitization	Multi-step	Crypto, Block-Erase, Device Overwrite + Verify	YES
UK CESG/GCHQ HMG IS5	3-pass	Zeros, Ones, PRNG + Verify PRNG	YES
US Air Force AFSSI-5020	3-pass	Zeros, Ones, PRNG + Verify PRNG	YES
US Army AR 380-19	3-pass	Random, Zeros, Ones + Verify Ones	YES
US Navy NAVSO P-5239-26	3-pass	Zeros, Ones, PRNG + Verify PRNG	YES

Teraware is certified by the Asset Disposal & Information Security Alliance (ADISA), Threat Matrix Level 2, for both SSDs and HDDs. This means that Teraware reporting requirements exceed many different audit requirements and compliance regulations for handling patient data, cardholder data, user data and data privacy, as well as those for industries regulated by the Securities and Exchange Commission (SEC)

Teraware engine

The Teraware platform centers its features around the agent engine. The agent engine conducts discovery to gather attributes for the target machine, controller and devices.

Each storage device and storage controller implements a standards based protocol that consists of mandatory and optional commands (i.e., commands that the device manufacturer may or may not implement). As part of the device discovery process, Teraware examines the controller-disk relationship to determine the preferred set of media sanitization commands supported by that specific device/controller combination. If those commands are either unsupported or simply unsuccessful, Teraware implements additional fallback protocols and will issue a known working command set instead.

Deployment services

Teraware is built on top of a custom Linux kernel with essentials, security patches, locked-down ports and an application layer that allows for the agent to be used in many environments.

Agent support for high-security deployment:

- HTTPS support
- IP table support
- User password set function
- User authentication with the API
- IPv4/IPv6 static or dynamic support

Reporting

Iron Mountain has gained valuable insights from our diverse customer and industry base, which has allowed us to refine our asset and job reporting practices. We've consolidated these varied requirements into best practices for reporting. Teraware's job reports and certificates meet audit standards like PCI, HIPAA, and SOX. Every storage device is tracked with detailed parent-child data, covering everything from the drive slot to the host asset, rack unit, floor location, rack serial number, and data hall, especially for onsite data sanitization projects.

For additional reporting requirements, the following data are available:

- Site location of the sanitization job
- Operator name, e-mail, phone number and role
- Host asset information (manufacturer, model, BIOS revision, CPU/RAM, asset tag, serial number)
- Disk device information (manufacturer, model, capacity, type, power-on hours, reallocated sectors, SMART status, disk slot)
- Sanitization standard used, result, start time, completion time, elapsed time, and device power-on hours at the end of the sanitization
- Teraware tool information such as product name, version and build info
- Teraware license holder information Iron Mountain declaration (for CoS), a statement that offloads liability from the customer to Iron Mountain. If a report or certificate does not offer any such statement of exemption from liability, then there is no transfer of liability and it is just a report.

More comprehensive information and health attributes are available through detailed reporting.

Audit trails

Teraware adheres to the highest regulatory compliance by creating a fully transparent and traceable audit trail for each serialized asset—from sanitization through disposition.

The auditing process has five steps:

1. **Complete an inventory scan**
   Teraware discovers every functioning asset, including location, condition and parent-child relationships.
2. **Sanitize all drives**
   Teraware fully erases all drives simultaneously regardless of quantity.
3. **Generate an automated report**
   Teraware generates a report and CoS for every erased drive.
4. **Scan and compare**
   Assets for resale arrive at an Iron Mountain facility to be scanned and cross-referenced with the generated reports.
5. **Remarket or physically destroy**
   Iron Mountain inventories assets for resale or provides Certificates of Destruction for shredded drives. Iron Mountain follows National Association for Information Destruction (NAID) requirements for physical destruction.

The Iron Mountain Web Inventory Tracking System (WITS) ensures that every asset is traceable at every stage and maintains parent-child relationships between each serialized asset.

Front-end interface

There are primarily two types of operators for Teraware:

1 **An operator** who manually controls the process workflow of assets and disks

2 **An automation framework** that follows predefined workflows

For the technician, Teraware offers a graphical user interface that allows the operator to group selected equipment and associate it with a predefined job template and processing policy. This is designed for simplicity. Technicians can navigate the operational workflow easily, and the solution requires very little training. Teraware does all the heavy lifting.

The automated solution offers a lightweight image with only an API interface that is used to manage Teraware.

Back-end interface

With the Teraware appliance and USB products, there will be a Teraware server on one machine communicating with Teraware agents on the targeted assets. There is no way for an operator to manage an agent directly. As a result, all requests are processed through the Teraware server instance using in-transit encryption remote procedure calls (RPCs) to the agents.

Teraware server has successfully processed as many as 9,160 servers with 45,579 disks under a single Teraware job. In this instance, the Teraware Enterprise Appliance used only an Intel i5 4-core processor, 16GB RAM and a single 1Gb Ethernet interface. The small footprint of running services increases the security of our solution while also allowing the operational environment to fully optimize itself to make the best use of CPU, memory and network interfaces within the Teraware solution.

Record keeping

Iron Mountain uses local and remote repositories for storing job reports and certificates. The local storage is used for running jobs and storage of all reports and certificates for the life of the appliance.

When Teraware completes a job, data may optionally be pushed to the Iron Mountain hosted enterprise endpoint servers and then replicated to a backup data center.

Enterprise features

Asset reconciliation and tagging

For many customers, the reconciliation of assets within a data center space may be a higher priority than the sanitization itself. The very first step of decommissioning is determining expected assets within the environment and then having a true confirmation that every asset and data-bearing device has been accounted for.

Teraware has an asset tagging and reconciliation feature. The starting point is uploading a prepared asset list into Teraware allowing for generation of a reconciliation. This allows the operator to export the report to find a list of reconciled statuses for each expected asset and identify unexpected assets. At this stage, the technician determines if troubleshooting is necessary for undiscovered assets/disks before initiating the sanitization job.

All reports will "tag" location attributes for each asset and disk device that will allow the technician to quickly find a failed or undiscovered disk within the data center floor by first locating the row/rack position, the rack unit where the asset is expected to be installed and the node position.

The reconciliation index can be based on

- System MAC address
- System BMC MAC address
- System serial number
- System programmed asset tag
- Disk serial number

Sanitization of storage components can proceed after reconciliation is complete. After the sanitization is complete the system presents the following information:

Undiscovered asset

These assets were not discovered by the sanitization tool but have been confirmed present and likely contain storage devices.

Undiscovered discs

Assets have been discovered by the sanitization tool, but the number of expected disks differs from the discovered disks under the asset.

Failed disks

These disks were part of the expected asset's inventory but did not complete the sanitization tasks successfully.

Sanitized disks

These disks were part of the expected asset's inventory and did complete the sanitization tasks and met all criteria for being issued the CoS.

Discovered assets not listed on the imported asset list are protected from data sanitization through a predefined Teraware policy. This policy ensures that assets with a "NON-CONFORMANCE" reconciliation status are excluded from processing and bypassed during sanitization.

Any storage devices not assigned a Certificate of Sanitization (CoS) should be treated as potentially containing sensitive data and thus need to be securely stored. These devices should be transferred from the parent asset into secure storage. Teraware offers tools and reports to identify drives that were not properly sanitized.

BMC reset

Among many enterprise organizations, out-of-band management (BMC/IPMI interfaces) of assets is configured with internal network configuration details and hostname structures. Teraware can sanitize the baseboard management controller (BMC) network configurations, hostname and user accounts. As Teraware is a job-based platform, a job report will be automatically generated that will show which assets were successfully processed for BMC resets and which ones were unsuccessful.

Asset tag sanitization

Teraware may be used to clear any programmed asset tag fields as part of the BMC reset task.

UID and SES LED support

For most servers, there is a locator mechanism called unit identification (UID). This is usually a blue LED on the front and rear of a server asset. When a Teraware job is started on the asset, it will clear the UID status and shut off the LED.

If a processed asset has failed disks, Teraware will turn on the system UID LED to help the technician locate the failed disk more quickly. Additionally, if the server contains a SAS expander, Teraware will use the SCSI Enclosure Services (SES) protocol to turn on the failed disk LED on the corresponding drive slot. The location features help reduce the time on the data center floor

Encrypted disk handling

There are many types of systems and disks within an enterprise fleet. Some assets will use full disk encryption, whereas others will not.

A few things to know about encrypted disks:

- In most cases, a server purchased directly from an OEM that has self-encrypting disks will not actually have encryption enabled. This is especially true if the server is ordered with an operating system installed. This is primarily due to the security aspects of key management and user-side passphrases. This may cause confusion when people think their data is encrypted between the disk and the controller, but usually it is not.
- Any disk that is sanitized under a controlled security process must be auditable after the sanitization from within a separate system. If a server has been deployed with encryption enabled between the disk and the controller, then that disk will only be accessible within that server. If the disk fails during the service life and is then pulled and processed for sanitization, it will fail immediately because the security protocol is enabled. This means that it no longer has the relationship with the controller.
- If the server with security-enabled disks is decommissioned in a situation where all disks received a CoS, any disk pulled for audit will fail. This is because the final media disposition will not be read logically. If the physical media was readable, then it will contain garbled characters that will result in inconclusive data recovery.
- Disks that have security protocol enabled can become usable in other systems after a TCG cryptoerase + revert function.

Before a Teraware sanitization job is run against an asset with security-enabled disks, the operator must upload a CSV file into Teraware that contains the disk's Physical Security ID (PSID).

What is PSID?

PSID stands for Physical Security ID. Because the PSID is a physical label, it cannot be read logically by software. This means it cannot be compromised by a man-in-the-middle attack. Physical access is required to read the PSID.

A preprocessing job will then confirm that the disks selected match the serial numbers uploaded and that the PSID format is correct. Once confirmed, the job will issue the TCG cryptographic erase and subsequently use the REVERT operation with the PSID to turn off the security protocol. Upon completion, the disks can be processed for media sanitization. If the sanitization is successful, the disk can be audited at any time within any system.

Disk health assessment

As part of the sanitization process of the disk or flash device, we collect valuable health attributes and media information throughout the sanitization. Reallocated sectors and read/write error rates are monitored on electromagnetic media and failed program/erase cycles on flash media. At the end of the sanitization, Teraware knows the integrity of the medium and can proceed to measure other aspects of the disks for performance and health attributes.

At the end of the diagnostics, Teraware will compare results against the customer's predefined thresholds (enforced by policy controls) to determine if the disk is eligible for reuse.

Teraware disk health assessment runs the following checks:

- Short or extended SMART test
- Sequential READ
- Sequential WRITE
- Random READ using 4KB blocks then records average IOPs
- Random WRITE using 4KB blocks then records average IOPs

For the sequential performance indexing, the profiling starts from the middle of the disk rather than the outer diameter of the disk. The reason for this is that showing the peak performance may not be a practical representation of the disk's longevity.

Through the policy controls, the block sizes can be defined for sequential and random IO performance profiling. Also under the policy, the predefined thresholds can be set to determine the SUCCESS/FAILED criteria of the assessment:

Power-on hours	<24,000 (default)
Reassigned sectors:	<3 (default)
READ throughput (MB/s)	>70 (default)
WRITE throughput (MB/s)	>70 (default)
Random READ (IOPs)	>80 (default)
Random WRITE (IOPs)	>80 (default)

Serial number normalization

Mismatched disk serial numbers can create challenges for auditing and asset inventories. To address this, Teraware uses a rule table that normalizes the discovered serial number, ensuring it aligns with the physical label serial number where possible. This helps maintain accuracy and consistency in asset tracking.

Performance optimizations

Processing performance rates are typically influenced by system architecture, disk read/write speeds, and disk quality. Speeds may decrease when processing storage servers with multiple disks on a shared data bus. Teraware optimizes performance with intelligent I/O processing, ensuring maximum speed while maintaining complete data sanitization integrity.

Error recovery

When encountering a disk with WRITE or READ issues, Teraware performs a set number of retries, attempting to clear data from these problematic devices. This approach aims to increase successful sanitization rates and achieve higher overall yields.

Drive discovery

When a Teraware agent starts, it will scan the device bus to determine the attached devices to gather parameters and capabilities for each of the connected storage devices.

Solid State Drive sanitization

Iron Mountain has invested extensively in research and development to create a robust SSD sanitization method that incorporates industry-standard protocols, error recovery methods, performance optimizations, and safeguards. This approach ensures the integrity of sanitization processes for flash-based storage devices.

Creating sanitization policies

The following section highlights key configurable features within Teraware for creating new policies.

Sanitization effectiveness (trade off for speed)

Firmware sanitization safeguard

Teraware implements safeguards in the task operations that make use of the firmware commands.

Teraware writes several blocks of a repeating pattern to seed the drive before the firmware command is issued. Once the application issues a firmware sanitization command to the device, it will then poll the device's command register for progress until completion. To verify the success of the firmware commands Teraware reads back the seed locations and compares them to what was written before the operation. If the data is still present Teraware will fail the task. If the seed data is not the same, it is confirmed that the firmware command changed the data on the device.

Sampling

This refers to the percentage of the disk that is to be verified as sanitized.

Mismatch blocks

Users can set a limit on the number of blocks that do not contain the expected pattern during the verification process before Teraware fails the task.

ERC write/read

Users can configure the amount of time a hard disk's firmware can spend recovering from a read or write error. (ATA drives only)

Create signature type

Allows users to create a signature on disk for later verification in another Teraware appliance.

Drive Quality

Max bad blocks

User adjustable threshold for number of blocks returning an error before a task is failed.

Reallocated sector threshold

Threshold used during disk diagnostic testing to pass/fail drive based on reported value.

Conclusion

The Teraware platform is verified and trusted by data centers, hyperscalers and Fortune 100 companies. No audit or forensic analysis has ever found any data on any electromagnetic or flash storage device that had been processed by Teraware.

IRON MOUNTAIN®

800.899.IRON | ironmountain.com

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 more than 90% 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.