Data Destruction

Data Destruction Overview

Data Vista's data destruction services for storage media ensure data cannot be retrieved or recovered. Data Vista's Data Destruction services enable our customers to be assured that whenever a technology device with a storage capability is designated for data destruction, the data is irretrievable. The process complies with the following criteria:

- meets corporate, industry, or government compliance standards for data destruction
- meets security policies as set forth by customer's security organization and/or auditors
- documentation of data destruction is properly recorded for audit and/or legal purposes

Data Destruction Capabilities

As storage media devices are decommissioned, re-purposed, or re-allocated, data must be effectively removed without traceable evidence from storage media. Data Vista uses the term "data destruction" to refer to any process where data must be removed by any appropriate process. We are able to perform data destruction for our clients to assure confidential or harmful information is never exposed to unauthorized sources.

Compliance Standards

To meet corporate, industry, or government guidelines, Data Vista complies with various standards and practices as documented in the following sources:

- National Institute of Standards and Technology document (NIST), NIST 800-88 Guidelines for Media Sanitization
- Department of Defense standards to include the NISPOM 5022.22M, "Defense Security Service Clearing and Sanitization Matrix"
- Individual client security company standards

Onsite or Offsite Data Destruction

Based on customer requirements, Data Vista can perform any of the above services onsite at customer premises, or offsite at a Data Vista facility in NJ. If offsite data destruction is utilized, we collaborate with the customer to offer or negotiate a secure Chain of Custody process to meet customer data security policies and procedures.

Documentation

Data Vista provides a Certificate of Data Destruction (CODD) to attest to destruction of data from media. For legal and/or internal audit purposes, a Certificate of Data Destruction (CODD) report includes:

- Unique property identification, in most instances a serial number, if available
- Time and date of sanitization
- Description of the media technology
- Disposition of the information technology resource
- Identity of individual executing the procedure
- Signed and dated documentation

Data Destruction

Data Destruction Overview

Data Vista's data destruction services for storage media ensure data cannot be retrieved or recovered. Data Vista's Data Destruction services enable our customers to be assured that whenever a technology device with a storage capability is designated for data destruction, the data is irretrievable. The process complies with the following criteria:

- meets corporate, industry, or government compliance standards for data destruction
- meets security policies as set forth by customer's security organization and/or auditors
- documentation of data destruction is properly recorded for audit and/or legal purposes

Types of Data Destruction

Data Vista Data Vista employs several methods for data destruction depending on the customer's objectives.

Clearing

Also known as overwriting, clearing preserves the media for re-use after data destruction via a software process has been applied. A binary [0/1] is written across all media locations and repeated at a minimum of 3 passes. Any data that was resident on the hard drive is untraceable and irretrievable. Upon completion of software process, random hard drives are tested to ensure no data is present.

Purging

Purging utilizes a degaussing device to remove data without the possibility of recovery. After being purged, hard drives can't be reused and are deemed as recyclable material. Degaussing emits a magnetic field resulting in the complete disruption of the hard drive's stored magnetic patterns and domains. The end result is untraceable and irretrievable data. Data Vista's degaussing equipment far exceeds minimum required specifications by most standards. Upon completion of degaussing process, random hard drives are tested to ensure complete erasure of data.

Physical Media Destruction

Physical Media Destruction is performed by shredding, pulverizing or hole-punching to completely destroy storage media and therefore any data it contains. The by-product (shredded material) averages in size to 1/8 inch and is recyclable material.

Types of Media for Destruction

Data Vista can destroy data on any of the following media:

- Disk drives, any OEM and any disk technology; SCSI / UW SCSI, SAS, SATA, Fibre Channel, IDE etc..
- Optical disk platters
- Tapes
- Cell phones
- Solid State Devices