1.0 PURPOSE

Disposition and sanitation are key elements for assuring confidentiality of customer data that resides on media returned to Quantum repair operations. This document provides clear direction for how to disposition and sanitize customer returned media.

2.0 SCOPE

This procedure applies to media that is returned as the result of service activity and that is processed by Quantum repair operations. The media types addressed in this procedure include magnetic tapes, HDDs, and SSDs.

3.0 REFERENCE DOCUMENTS

3.1 NIST Special Publication 800-88, Guidelines for Media Sanitization

3.2 NIST Special Publication 800-36, Guide to Selecting Information Technology Security Products

4.0 DEFINITIONS

4.1 HDD – Hard Disk Drive used in Quantum disk-based backup systems.

4.2 SSD – Solid-state Drive used in Quantum disk-based backup systems.

5.0 BACKGROUND

5.1 Sanitation Methods (Reference: NIST Special Publication 800-88, Guidelines for Media Sanitization)

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36]

Destroy	There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. • *Disintegration, Pulverization, Melting, and Incineration.* These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • *Shredding.* Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm^2).

NOTE: Per NIST 800-88, Secure Erase is an acceptable overwrite method for clearing and purging data.

5.2 Secure Erase Command

5.2.1 The International Committee for Information Technology Standards (INCITS) is the forum for creation and maintenance of formal IT standards. INCITS is accredited by, and operates under rules approved by, the American National Standards Institute (ANSI).

5.2.2 Technical Committee T13 of INCITS is responsible for all interface standards relating to ATA storage interface utilized as the disk drive interfaces.

5.2.3 The ANSI T13 committee added the Secure Erase (SE) command to the ATA interface specification (also called IDE).

5.2.4 The SE command is implemented in all ATA interface drives that are greater than 15 GB and that are manufactured after 2001.

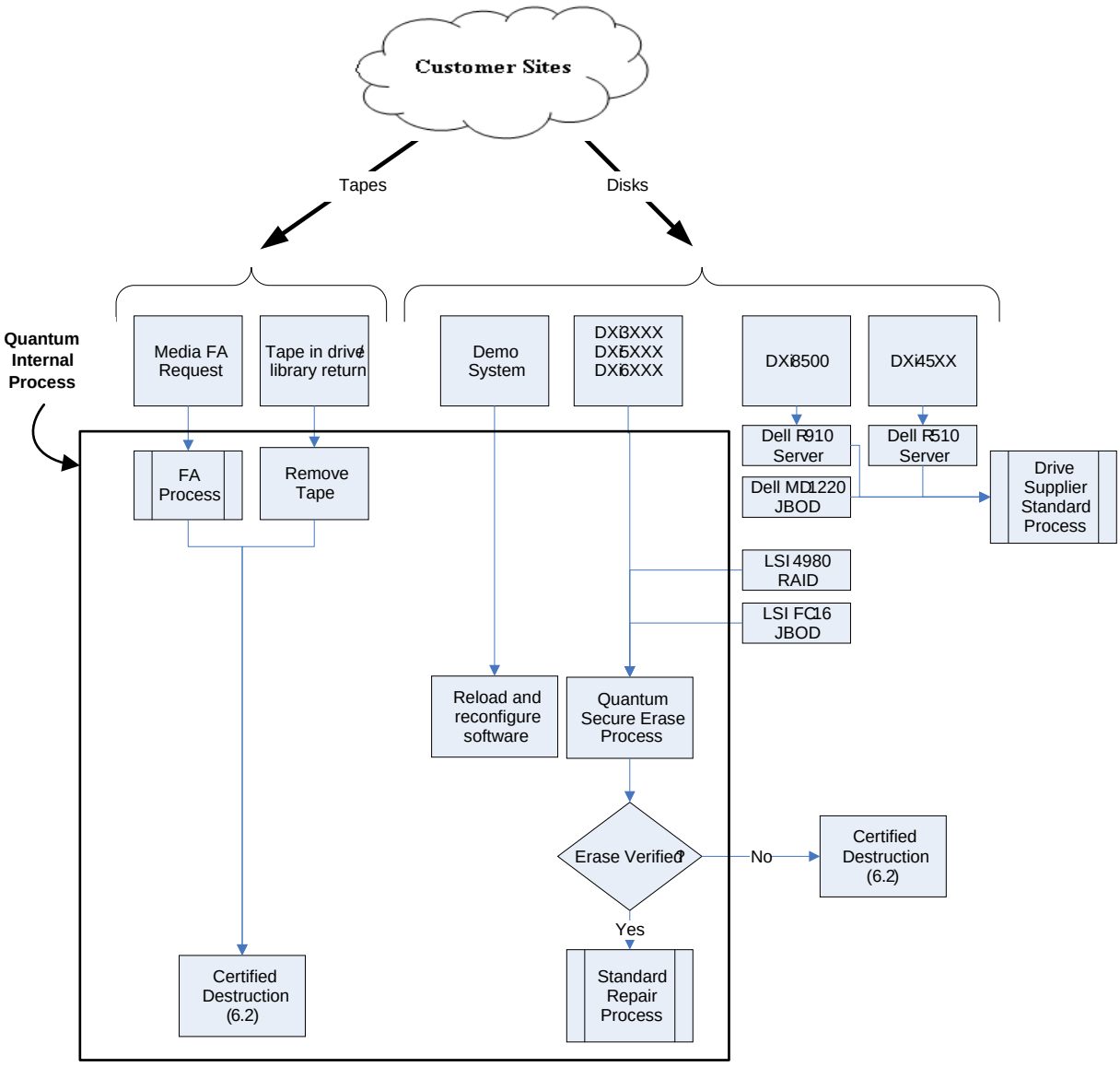
5.3 Quantum Implementation for Secure Erase

5.3.1 A Quantum test system shall execute the Secure Erase command that is built into the HDD or SSD firmware or perform an operation that provides equivalent functionality.

5.3.2 If an equivalent function is implemented, the software and effectiveness shall be verified through a documented validation report.

6.0 PROCEDURE

6.1 Process flow



6.2 Certified Destruction method

6.2.1 The media (tape, HDD, or SSD) is placed into a secure, locked cage.

6.2.2 Once the cage nears capacity, an industrial recycler is scheduled.

6.2.3 A Quantum employee, or designated representative, accompanies the media to the recycler facility, unlocks the cage, and witnesses the destruction.

6.2.4 A Certificate of Destruction from the industrial recycler is obtained and retained for each batch of media that is destroyed.

6.2.5 For HDDs and SSDs only, a list of serial numbers destroyed shall be attached to the certificate of destruction.

7.0 RECORDS

Traceability for the serial numbers of the drives (HDD and SSD) that are processed through the secure erase process will be maintained through the Quantum KIOSC system. If an HDD or SSD is destroyed, then a list of serial numbers is attached to the certificate of destruction and maintained in hard copy format.

Records Identification (Title of record. Example: DVT Report, ECO, etc.)	**Location** (Where are records stored?)	**Category** Hard Copy – enter the Record Description found in QF00155 Soft Copy – enter Soft Copy	**Retention** Hard Copy - see QF00155 Soft Copy - governed by IT system backup and retention processes
Process Test Record	KIOSC DB	Soft Copy	governed by IT system backup and retention processes
Cert. of Dest.	Media Quality Dept.	Legal - Archive logs, destruction records…	see QF00155