

Scope

This document describes the processes used by Carrier Services Group, Inc. (CSG) to destroy data on **hard disk drives (HDDs)** and **solid-state devices (SSDs)** received from Data Controllers. CSG performs both logical data sanitization and physical data destruction at its facility using qualified, trained personnel.

1. Receipt & Secure Handling

Upon receipt, all data-bearing devices are inventoried with date received, client identification, item count, and traceability identifiers (e.g., contract number, BOL, shipper number). Devices are moved to a secure, access-controlled storage area and remain under documented security controls until destruction is complete. Surveillance is maintained in all areas where data-bearing media is stored, wiped, or destroyed.

2. Logical Data Sanitization (HDDs & SSDs)

Devices designated for logical sanitization are processed using **KillDisk** sanitization software, compliant with the **NIST 800-88** standard (All Zeros method). The software captures the serial number of each device and generates an erase certificate upon successful completion. Devices that fail the logical sanitization process (due to drive failure, connectivity issues, or inability to be read) are automatically routed to physical destruction. **Validation:** A minimum of 1% of logically sanitized devices are validated using a separate software manufacturer to verify the effectiveness of the sanitization process, in accordance with R2 and NAID AAA requirements.

3. Physical Data Destruction (HDDs & SSDs)

Devices designated for physical destruction — including any devices that failed logical sanitization — are processed using an **SEM shredder**. The shredder is operated by trained personnel and is under surveillance throughout the destruction process. Serial numbers of all devices are recorded prior to destruction. The shredder reduces devices to a particle size that renders data unrecoverable. Both hard disk drives and solid-state devices are destroyed through the same shredding process.

4. Documentation Provided to Data Controllers

Upon completion of destruction, CSG provides a **Certificate of Destruction** to the Data Controller documenting the devices processed. All destruction records are maintained by CSG for a minimum of three (3) years.

5. Personnel & Quality Controls

All data sanitization and destruction activities are performed by qualified personnel who have received documented training. CSG conducts annual internal audits and data sanitization audits for conformance to R2 Appendix B and NAID AAA requirements. All data sanitization is completed within two (2) months of receipt of devices.