DATA DESTRUCTION BEST PRACTICES
FOR END-OF-LIFE (EOL) MEDIA HELD IN-HOUSE

To ensure the security and confidentially of sensitive data on EOL storage media physically located at your facility, it is essential to implement the following data destruction best practices:

1. **Prioritize secure handling and maintain chain-of-custody.**

   As the collector of data, you hold the sole responsibility for upholding the security and confidentiality of all sensitive data forever. This responsibility cannot be transferred to a third-party IT asset disposition (ITAD) vendor. The collector of data remains fully accountable and liable for any potential data breaches or security incidents that may occur.

2. **Perform in-house data destruction.**

   No EOL storage media should ever leave your facility or be released to a third-party vendor without undergoing an in-house data destruction process.

   Hard disk drive (HDD) storage media must go through an in-house degaussing process. Degaussing destroys 100% of HDD data rendering the data irretrievable. Solid-state drives (SSDs) require physical destruction as they store data electronically on flash memory chips. Proper physical destruction of the chips on solid-state drives makes data recovery impossible.

3. **Generate a Certificate of Destruction (COD).**

   A COD is an essential document that provides concrete evidence of proper, secure, and comprehensive data destruction for the data storage media, ensuring a complete EOL media audit trail.

   For **HDD**: Obtain and maintain a detailed record of the degaussing process including media serial/asset numbers, operator ID, date, time, location, degausser field strength applied to the media, and specific information about any physical destruction performed for every single drive.

   For **SSD**: Obtain and maintain a detailed record consisting of the serial number, a photo of the media, and diagnostic data from the destroyer, including crush depth and media type, for every single drive.

4. **Release the EOL storage media.**

   The EOL storage media can leave your facility or be released to a third-party ITAD only after steps one through three have been successfully completed.

Visit garnerproducts.com for a range of custom data destruction packages or contact Chris Trevino at chris@garner-products.com.

Garner Products, Inc.
10620 Industrial Avenue, Suite #100 Roseville, CA 95678 USA.
Toll Free: 800-624-1903 | info@garner-products.com
www.garnerproducts.com

DATA DESTRUCTION BEST PRACTICES CHECKLIST FOR MEDIA HELD BY THIRD-PARTY DATA STORAGE PROVIDER

If you rely on third-party data storage providers, cloud services, or co-location facilities and find yourself unable to perform in-house data destruction processes, it is imperative that you demand transparency and thoroughly assess the end-of-life (EOL) data destruction protocols before selecting a service provider.

As the collector of data, you still hold responsibility for upholding the security and confidentiality of all sensitive data, in perpetuity. This responsibility cannot be completely transferred to a third-party IT vendor. You, the collector of data, remain forever accountable and liable for any potential data breaches or security incidents that may occur.

To help you in your assessment, we have developed a comprehensive checklist that you can use as a reference. The following checklist is intended for the third-party data storage provider being evaluated for their EOL data destruction processes.

1. Data Destruction Processes:

- ☐ Provider employs an in-house degaussing process for HDD and physical destruction for SDD. If yes, proceed on to checklist item number 2.
  [**NOTE**: These are the only acceptable and most secure EOL data destruction processes. If the potential service provider does not employ degaussing (HDD) or physical destruction (SSD), do not proceed.]
- ☐ Provider implements overwriting as the means of data destruction. **STOP**.
  [Note: If the provider answers yes to this question, you are at risk. Overwriting is not a secure data destruction method. Overwriting can leave sectors of sensitive information intact, vulnerable to retrieval and data breaches.]
- ☐ Provider sells decommissioned hard drives on the secondary market. **STOP**.
  [Note: If the provider answers yes to this question, you are at risk. Although promoted as environmentally friendly, these overwritten or encrypted hard drives still have intact sensitive information, vulnerable to retrieval and data breaches.]

2. Certifications and Compliance:

- ☐ Provider has certifications or third-party audits validating data destruction practices.
- ☐ Documentation or evidence supporting compliance claims can be provided.

3. Documentation and Auditing:

- ☐ Detailed documentation outlining the data destruction process is available.
- ☐ Provider tracks and documents the destruction of physical media and storage devices.
- ☐ Regular internal or external audits of data destruction procedures are conducted.

4. Verification and Proof:

- ☐ Provider provides proof or verification of irretrievable data destruction for every single drive.
- ☐ Certificates, reports, or other evidence demonstrate successful completion of data destruction for every single drive.

5. Subcontractors and Subprocessors:

- ☐ Provider engages subcontractors or subprocessors for data destruction purposes.
- ☐ Assurance is given that subcontractors adhere to stringent data destruction standards.

Garner Products, Inc.
10620 Industrial Avenue, Suite #100 Roseville, CA 95678 USA.
Toll Free: 800-624-1903 | info@garner-products.com
www.garnerproducts.com

6. Chain of Custody:

- ☐ Provider explains chain of custody procedures for physical media and storage devices.
- ☐ Provider ensures secure handling of data from its departure until permanent destruction.
- ☐ Secure transportation methods are used for transferring physical media.

7. Employee Screening and Training:

- ☐ Provider ensures trustworthiness and reliability of staff handling data destruction.
- ☐ Security measures are in place to prevent unauthorized access during data destruction.
- ☐ Background checks are conducted on employees.

8. Disaster Recovery and Business Continuity:

- ☐ Measures are in place to ensure operational continuity during disaster scenarios.
- ☐ Protection against data breaches, physical damage, or data loss in unforeseen events is implemented.

Garner Products, Inc.
10620 Industrial Avenue, Suite #100 Roseville, CA 95678 USA.
Toll Free: 800-624-1903 | info@garner-products.com
www.garnerproducts.com