# Destruction Fact Sheet

Thank you for trusting A&G Electronics with the secure destruction of your devices. This sheet explains the process applied to your equipment based on the service option you selected.

## 🔹 If You Selected Data Destruction (Digital Wipe)

- Devices that **qualify for reuse** (i.e., fully functional and able to pass testing) are securely wiped using **NIST 800-88r1 standards**.
- For **HDDs (Hard Disk Drives):** all data on the platters is overwritten multiple times until it cannot be recovered.
- For **SSDs (Solid State Drives):** a specialized data purge method is used to clear all data cells.
- Devices that successfully pass this process may be refurbished and reused.

👉 **Important:** If any device submitted for data wiping does not meet reuse standards (damaged, faulty, or cannot be fully sanitized), it is **automatically physically destroyed** to ensure your data security.

## 🔹 If You Selected Physical Destruction

- All devices, whether functional or not, are mechanically destroyed.
- Methods include shredding, crushing, or dismantling until all storage components are permanently unusable.
- This method guarantees complete data security and is often required for customers subject to stricter compliance (e.g., HIPAA, ITAR, DoD).

## 🔐 Key Notes

- **Data Destruction** = reuse possible, but only after secure wiping. Non-reusable devices are physically destroyed.
- **Physical Destruction** = no reuse possible; all devices destroyed regardless of condition.
- Both methods ensure that **no recoverable data remains**.

## ✅ Your Assurance

- All services are carried out under A&G's secure destruction policies, modeled after **NAID AAA Certification standards**.
- Devices are tracked under a documented chain of custody from intake through final processing.
- A **Certificate of Destruction** will be issued separately for your records via email.