Data Destruction Checklist

CEAR

As our reliance on data grows, it is increasingly important to safeguard customer information. Protecting and ultimately disposing of the physical hardware should be carefully planned, and choosing the method and vendor that suits your requirements is critical to preventing unauthorized access of information.

Complete our data sanitization checklist to review your disposal procedures and policies.

Policies and Regulations

□ Check legal and regulatory requirements that may apply to your organization.

□ Ensure your policies for data security include physical equipment protection.

□ Train employees on data security and record retention policies

Equipment

□ Decide how data storage will be destroyed based on the needs of your organization.

o Physical destruction: shredding prevents access to data stored on hardware

o Wiping and Overwriting: Data is unrecoverable but hardware can be reused

□ Ensure all other device data is wiped or destroyed during recycling or before resale.

Vendors

□ Choose a vendor who is Certified and independently audited

o R2 and E-Stewards certify organizations for secure E-Waste Recycling

o NAID AAA data destruction Certification satisfies regulatory due diligence.

□ Choose a vendor who offers the services your organization requires, such as:

o Onsite shredding or wiping

o Facility-based Shredding or wiping

o E-waste recycling with data sanitization

□ Ensure your vendor can track devices in transit and provide chain of custody records

□ Choose one vendor for electronics recycling and data destruction to control liability

□ Ensure the vendor can provide certificates of destruction, video, and serial numbers to create audit trails

CEAR, being a certified vendor for NAID AAA and R2, has the capabilities to assist your organization in developing a compliant data destruction solution.

☎ (916)-388-1777 ✉ info@cearinc.com 🌐 cearinc.com