Destroying Information on Retired Electronic Equipment

THE CHALLENGE:
Knowing Your Risks and Obligations

Why Information on retired computers must be properly destroyed.

- IT'S THE LAW - There are strict laws requiring you to prevent unauthorized access to the personal information on discarded computers.

- FINES - Over the last 2 years alone, there has been in excess of $10,000,000 in fines for improperly discarding sensitive personal information, not to mention scores of embarrassing headlines.

- BREACH NOTIFICATION — Legally required notification of clients when there is a data breach can cost tens of thousands of dollars and much, much more in lost customer confidence and future business.

- ETHICS - You have an ethical obligation to your clients and stakeholders to properly destroy personal and proprietary information when discarding or transferring ownership of old computers.

* Each of the listed information destruction methods come with specific distinctions. Even if a potential contractor does not offer all these methods of information destruction, they should be able to explain the relative advantages and disadvantages of each.

THE SOLUTION:
Using A Qualified Contractor

WHY OUTSOURCE?

Information destruction methods for computers are best left to someone who knows what they are doing. Even professionals have to recheck their work with forensic systems to verify destruction. Self-administered procedures are far more likely to be ineffective. Further, authorities do not look kindly upon those who cut corners on information destruction.

THE MOST IMPORTANT DECISION

When decommissioning old computers, your most important responsibility is to make sure you are dealing with a reputable company that puts information destruction first. A qualified contractor will help you determine if Sanitization, Secure Erase, Degaussing or Physical Destruction is the best destruction process for any particular circumstance.*

FINDING QUALIFIED COMPANIES

Companies qualified to remove information from old computers with the assurance you need have some things in common.

- They encourage you to visit their operation even when it's a surprise.

- They effectively control unauthorized access to their facilities.

- They track the serial numbers on the computers and/or hard drives and have a complete physical and documented audit trail in place.

- They have a documented quality control program to verify the effectiveness of the destruction process on an ongoing basis.

- They have documentation that shows where they send the processed remains of the equipment.

- They screen their employees and do not employ individuals with a known related criminal history.

- They issue a certificate of destruction that addresses the "who, where, when and how" of the destruction process.

- They demonstrate their dedication to proper information destruction through membership in NAID.

NAID

Contact the following NAID MEMBER about protecting yourself, your organization and your customers with a high-security information destruction program.

NAID