

Protect Yourself

Certified Data Erasure Enables Security in Disposal Management Policy

Management of information technology (IT) assets is a complex task for any organization and an important effort in controlling IT costs. While maximizing asset use is important in achieving IT budgets, even greater costs are at stake if a company does not create and enforce an asset disposal management policy that protects data, the environment and regulatory compliance.

Disposal management is a critical subset of an effective information technology (IT) asset management strategy, with implications that extend far beyond the simple physical removal of an asset. To securely reassign, refurbish or remove an asset from service, a company should create a disposal management policy that includes these three critical processes: data erasure, software license harvesting and physical disposal. Each of these carries its own risks if not executed properly, but failure to fully erase data has the most serious consequences. Once data leaves the premises, there is no chance for protecting it.

Data breaches stemming from failure to erase sensitive corporate and consumer data before an asset changes hands are reported on a daily basis. An organization that fails to properly secure its business information when assets leave the premises risks severe penalties on a variety of legal, financial and public relations fronts. Combined with the need to secure data for compliance with PCI, HIPAA and other regulations, these risks designate data erasure as the first process for execution as part of a disposal management policy.

Despite the need for an effective disposal management policy, a 2005 IDC study suggests that only 37% of commercial entities have a formal PC recycling and end-of-life asset policy in place. In addition, for enterprises with operational data centers, managing these processes for IT equipment such as servers and storage arrays is even more demanding. The report also indicated that similar percentages apply to data destruction.

Certified data erasure software as described here is an important tool in the disposal management process and overall asset management strategy. Unlike other data destruction methods, it not only removes all data from an asset, but also

provides verifiable proof that meets all major regulatory and data removal standards.

In addition to data removal, certified data erasure supports effective license harvesting and physical disposal. However, before embarking on any type of data removal process, organizations must first develop sound policy surrounding it.

Disposal management requires sound data erasure policy

To mitigate the risks of information fraud while ensuring compliance with government regulations, privacy concerns, and intellectual property rights issues, it is the responsibility of every company to design effective data erasure policies and procedures for IT assets destined for disposal or reuse. Here are some important steps for creating a corporate-wide data erasure policy:

Pursue a practical approach

Each company's data erasure policy should be based on several business factors such as the size of the organization, the frequency of data erasure and disposal, and specific industry requirements. For example, purchasing expensive data erasure equipment may not be financially feasible for a small business. On the other hand, storing thousands of outdated computers is never feasible for a large enterprise since it can present a security risk. To determine the most effective solution, businesses should assess their existing resources and add outside expertise where resources are lacking.

Consider budget impacts

Most enterprises have a budget for IT equipment and services, but few have one for data erasure and asset disposal. While organizations may see data erasure and asset disposal as expenses, these processes can actually contribute to budgets by qualifying an asset for reuse or resale.

By deploying an effective data erasure strategy, an enterprise can often recoup the remaining value on equipment by reselling it around three years after acquisition. Usually, IT



assets are fully amortized in three years. The remaining remarketing value (RMV) is not related to amortization schedule. However, somewhere after three to five years (servers and storage hold their value longer) the RMV will go to zero (but the disposal cost remains) and the asset becomes a liability.

Assign responsibilities

Organizations must determine who makes the ultimate decision regarding data erasure. Is it a “C-Level” business executive, an IT Director or a Purchasing Manager? Data erasure is not a technical or operational issue; it is a risk and liability matter. As a result, the decision-maker should be the individual most impacted if something goes wrong, such as a corporate risk manager or security architect. In either case, data erasure is a process that requires an owner. Additional personnel matters include determining the number of people required for data erasure, where they will be located and what role Human Resources will play.

Pick a secure disposal facility

The facility where data erasure is performed can impact both the quality and security of the erasure process. For example, onsite data erasure provides the most secure option by ensuring that sensitive data doesn’t leave the enterprise. Using an off-site or third-party IT asset disposal provider (ITAD) to perform the data erasure adds steps to the process, which require verifiable facility security and documentation.

One effective option is to use a combined approach where both on-site and off-site facilities are employed. For example, an enterprise could designate unencrypted servers for in-house erasure, leaving laptops with safer full disk encryption for secure shipment to an ITAD.

Balance risk versus cost

Whether considering an internal employee or external company to perform data erasure, it is important to consider the factors of cost and control. A policy that uses internal employees or brings outside service providers on-site provides

the greatest control, but may incur higher costs. Shipping media to an off-site location affords a lower cost, but yields less control. Both options are viable, but risk versus cost considerations must be weighed.

Prepare for data center device management

Data center equipment is deployed, run and managed differently from desktop PCs and laptops. As a result, the process of removing storage devices designated for erasure from equipment like a network server or storage array can impact business functions.

Decommissioned servers or storage arrays are typically offline but still powered, which allows access to all areas of a disk to ensure full data erasure. Powering down a server or storage array for erasure at an offsite facility jeopardizes access to the entire disk in case the ITAD cannot revive the operating system. In-house erasure is the most secure and least time consuming option, but often requires in-depth knowledge of a specific product line. Because of this, it is often more cost-effective to bring in qualified experts rather than risk partial or no erasure by inexperienced employees.

Research regulatory and reporting requirements

A host of strict industry standards and government regulations require organizations to mitigate the risks of unauthorized exposure of confidential data. Organizations in regulated industries must research which regulations apply to them and what requirements those regulations have for data and IT asset disposal. Examples of pertinent regulations include:

- HIPAA (Health Insurance Portability and Accountability Act)
- FACTA (Fair and Accurate Credit Transactions Act)
- GLB (Gramm- Leach Bliley)
- CAL SB1386 (The California Information Practice Act).
- SOX (The Sarbanes-Oxley Act)
- PCI DSS (Payment Card Industry Data Security Standards)

Also, regulated companies that handle sensitive data must understand the necessity of producing a detailed report as evidence of steps taken to prevent leakage of confidential information. A verification report and certificate is a key requirement for many regulations.

Certified data erasure mitigates risks and addresses compliance

After the data erasure policy is created, organizations must select the most secure and effective way to implement the data erasure process and enforce the data erasure policy. Best-in-class certified data erasure tools use a method of software-based and/or firmware-based overwriting that completely destroys all electronic data on hard drives or other digital media by overwriting it with a pattern of 1’s and 0’s. Basic file deletion commands, for example, do not erase data and

only remove direct pointers to data disk sectors, making data recovery possible with common software tools.

Unlike degaussing and physical destruction, certified data erasure removes all information while leaving the disk operable. This preserves computers for resale and refurbishing and provides an environmentally-friendly alternative to physical destruction.

A certified data erasure tool can supply a detailed report as proof of erasure for compliance purposes, which physical destruction and degaussing do not provide. Reports include lists of the disposed or erased items, their serial numbers, software serial keys found on the disk, how the data was erased or the asset was destroyed, and the disposal procedure (s). The ability to produce these reports is a key advantage of certified data erasure software over other erasure methods that helps protect enterprises from compliance litigation.

Also, a certified data erasure tool has the capability to provide report data to an organization's asset management and tracking system. Companies often lose track of retired IT assets and more importantly, the data they contain. By sending data erasure reports to an asset management system, or the person designated for this task if a system isn't in place, organizations can keep track of retired systems they have sanitized. This also protects the disks or equipment slated for reuse/re-marketing, if that is the next step.

Many organizations, however, do not have data erasure software and so rely on an ITAD or erasure service for audit trails. If using a third-party for data erasure, it is important to understand the type and quality of erasure software it provides, as well as the availability of a detailed erasure report. However, many analysts advocate that disks are wiped both by the company and at the ITAD facility.

Risks and rewards related to software license harvesting

The failure to harvest software licenses does not carry as dire of consequences as losing sensitive data and intellectual property if an asset is not fully erased. However, application



or system software that remains on a hard drive when an asset changes hands may violate site-licensing terms from the software developer. Also, the reallocation of a server to another department or division can breach a software license and can incur costly fines.

Certified data erasure helps with software license management by identifying the main software serial keys on an asset as part of the data erasure report. The report provides verifiable proof that software has been removed and may be reassigned. This allows an organization to save on costs for new software licenses without worrying about violation of licensing agreements.

Proper physical disposal preserves environment and reputation

The importance of choosing a third-party that provides EPA-compliant physical disposal cannot be minimized, because old computers and other equipment can severely contaminate soil and water, pose risks to human health and leave an organization subject to fines and bad publicity. In addition to providing a detailed data erasure report with asset serial numbers for compliance verification and asset tracking, a third-party ITAD should adhere to zero-landfill and no hazardous waste export policies that provide for downstream recycling and material recovery.

When choosing a third-party to dispose of IT assets, an organization should look for facilities that are ISO 9001, ISO 14001 and OSHAS 18001 certified or operate under ISO compliant processes. Many companies represent themselves as recyclers or disposal companies, but fail to be transparent in their processes. The ITAD should be insured at a minimum of \$1 million and must be able to provide references. It should also have certified engineers for onsite support.

In addition to the previous considerations, the following are important questions to ask of a third-party ITAD:

- Does the location provide a Statement of Work (SOW) detailing the steps in their erasure procedures?
- Do they use proven software and operational techniques?
- Can they provide certificates for regulatory compliance reporting?
- Have they installed security cameras for surveillance in designated work areas?
- Do they use sealed and secure containers to prevent unauthorized access during shipping?

Markku Willgren
President, US Operations
Blanco LLC