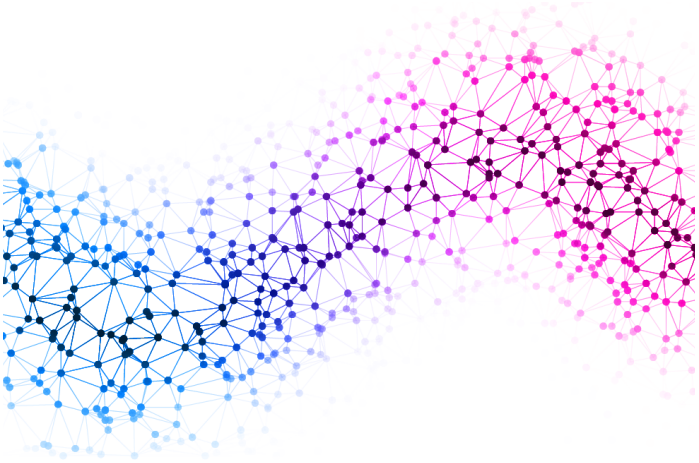
Best Practices in Drafting a Data Decommissioning Policy

SEM®

Global Leader in High Security Information End-of-Life Solutions for Over 50 Years

The amount of data that a company, agency, or individual possesses will continue to exponentially grow as time marches forward.



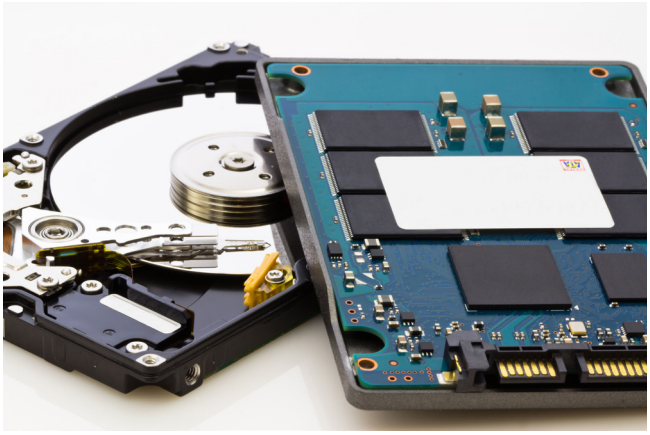
When drives reach their end-of-life through failure, technological obsolescence, or routine upgrade, organizations are faced with several choices on how to dispose of that data securely. It is imperative that any organization, agency, or business draft a data decommissioning policy that states best practices and detailed instruction for what to do when data reaches its end-of-life, ensuring that all data — from personally identifiable information (PII) to the government's top secret and classified data — does not fall into the wrong hands.

Drafting a Policy: Security First

When it comes to the destruction of classified and top secret information, the security of the data and complete confidence that the data has been properly destroyed should always be the main priorities. But what counts as being properly destroyed? The truth is, different industries, countries, and states have different requirements, including the following:

• *NSA Evaluated Product List (EPL)*: U.S. Government standards for top secret and classified data.
• *Payment Card Industry Data Security Standard (PCI DSS) Compliance*: Standards for the security of credit cards.
• *General Data Protection Regulation (GDPR)*: Regulations for businesses who operate with or within the European Union.
• *Personal Information Protection and Electronic Documents Act (PIPEDA)*: Regulations and standards for data privacy in Canada.
• *Fair and Accurate Credit Transactions Act (FACTA)*: Regulations for disposal of consumer information in the credit industry.
• *National Institute of Standards and Technolgy (NIST) 800-88*: Guidelines by the Information Technology Laboratory (ITL) for media sanitization.

Identifying regulations with which an individual organization must comply, both through legislation and by company requirement, is critical before a policy can be drafted. Once regulatory requirements are understood, organizations can research processes, equipment, and services to include within the policy. In addition, one critically important aspect needs to be prominently considered: the risk of data leaks.



As data management continues to become more complex, industries at large are searching for more efficient ways to destroy increasing volumes of data that expand across multiple forms of media. Paper, optical media, removable storage, rotational hard disc drives (HDDs), solid state drives (SSDs), and other types of electronic storage media can all be present in a single location. And as data management becomes more complex, data leaks become more prevalent. In recent years, it has become commonplace for organizations of all types — including small and large businesses, retailers, government agencies, healthcare companies, social media giants, cloud service providers, and municipalities, to name a few — to experience data leaks and breaches, with devastating effects to those whose information was compromised.

When drafting a data decommissioning policy, security — including complete elimination of sensitive data — is what should be at the forefront of the decision-making progress. And while there are numerous methodologies for eliminating sensitive data, such as shredding, disintegrating, erasing, and crushing, data destruction programs are much more straightforward in that they can be simplified to just two categories: in-house destruction and third-party destruction. But while they may be simple concepts, the pros and cons for each weigh heavily when making the best decision for a new data decommissioning policy.

Third-Party Destruction: Flexible, Easy, Less Secure

One common method for end-of-life data destruction is the use of a third-party company, commonly known as an IT Asset Disposition (ITAD) company. An ITAD will utilize their own data destruction devices to destroy sensitive media for an agreed-upon price. ITADs will either have organizations ship material to them or will come and pick up materials for destruction . There are also ITAD companies that transport destruction equipment in a truck, allowing destruction to be completed at the site that has requested destruction. One benefit of using an ITAD for data destruction is the fact that the agency or organization hiring them can be almost entirely hands-off. Assemble the media that needs to be destroyed, the ITAD destroys it, and the process is complete – no hassle.

Using an ITAD is an attractive option as there is no significant upfront cost to purchase a machine for data destruction, and it eliminates the need for any space requirements. However, it is important to note that a specific budget will need to be allocated as an ITAD is a recurring cost due to the inevitability of future failed or outdated media requiring destruction and replacement. ITADs can also be beneficial to organizations with larger volumes that do not have the personnel available to destroy the media in-house.

But despite the potential benefits for lower volume and smaller budget projects, ITADs come with a certain amount of risk that warrants extra consideration before investing in a partnership. When it comes to sensitive data, such as that containing personally identifiable information (PII), personal health information (PHI), top secret/classified information, or controlled unclassified information (CUI), the fewer people that handle the drive, the better. Hiring a third party inherently comes with a level of uncertainty that the media was destroyed to appropriate standards or that it was disposed of properly, as the organization responsible for the data is not performing or overseeing the destruction themselves.

A more concerning risk with third-party vendors is trustworthiness, mainly because the chain of custody greatly increases when using third party destruction. And, when it comes to sensitive data, each additional person who touches the data exponentially increases the risk, particularly when those people are not known, vetted employees of the organization housing the data. There have been instances of sensitive information being discovered on hard drives that were contracted to be destroyed by third party companies. These hard drives, whose owners paid to be destroyed, were only partially wiped and then put on eBay where eventual buyers found the data on the used hard drives. These cases, while isolated, represent a larger security concern with destroying data off-site. And while many companies in the ITAD industry declare integrity, it is important when going this path to find a company with a longstanding and impeccable reputation for integrity and honesty.

It is also important to remember that data removal on hard drives is not one hundred percent guaranteed when the drive is only erased and not destroyed. As an example, data recovery provider Kroll Ontrack was able to recover 99% of the data from the computer drive of the spaceship Columbia after the ship had exploded. If data can be recovered from a drive that went through an explosion, fell miles to Earth, then sat in a riverbed for six months, it's safe to assume data can be recovered from a "wiped" drive.

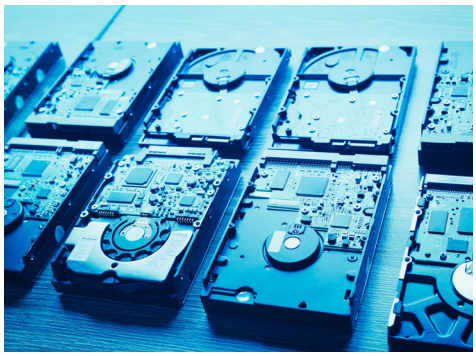
The drive recovered after the Columbia explosion

In the previous eBay story, the drives that were picked up were given to an ITAD with the agreement that they would be physically destroyed. Instead, the drives were only erased and resold to market, where the sensitive data was then recovered. If the drives had been erased and then physically destroyed, the margin for error and the chance of any data being recovered hovers a lot closer to zero.

In-House Data Destruction: Highest Security, Customizable, Requires Maintenance

The other methodology for data destruction is in-house, meaning that data destruction equipment is owned and maintained by the company housing the data. The main benefit of destroying data in-house — and it is a big one — is security. In-house data destruction is by far the most secure way to destroy data, as it casts the biggest safety net over a company, agency, or organization. Destroying data in-house significantly reduces the chain of custody, mitigating the risk of a potential leak or data breach due to recoverable data leaving the premises or being handled by any person other than a vetted employee. This sense of security and confidence of complete and thorough destruction or erasure cannot be overstated for many organizations that deal with PII and top secret data, as anything less than complete and total erasure could result in devastating losses.

When it comes to volume, there are numerous options for in-house destruction machines that correlate directly to the amount of data needing to be sanitized. For example, paper shredders and disintegrators are available at a variety of throughput levels and speeds that provide flexibility of having to shred a few documents or a room full of documents daily. Having low volume does not eliminate the possibility of bringing data destruction in-house, as destruction devices are available for even very low volumes and at very affordable price points that provide quick ROI.



Speaking of ROI, in-house destruction may appear to be more costly up front. Buying a machine will always be more expensive than using a service in the beginning; however, for organizations requiring medium to high volumes of destruction, dedicated machines often pay for themselves numerous times over during the years they are in use. Keep in mind, there will be continued costs. Data destruction devices require routine maintenance and service in order to continue to run effectively and efficiently for many years. But even with the ongoing cost of a service plan, in-house destruction devices still provide a positive ROI over their lifetime.

One other consideration when deciding between in-house or third party destruction is space. Data destruction units need designated space, and, again depending on volume, some organizations may not be able to physically fit the machine(s) that they need. In addition, larger hard drive shredders and paper disintegrators can be somewhat noisy and messy if sound mitigation and/or filtration options are not included with the device. A reputable and knowledgeable device manufacturer works with organizations to understand budget, volume, space, area, and availability of personnel to provide the best solution to fit these needs.

Making the Data Destruction Decision

While drafting a data decommission policy, ultimately either in-house destruction machines or the use of ITADs and third parties will be chosen as the solution for end-of-life of data. So, what is the correct answer? Now that each data destruction method has been broken down, it is important to consider three questions to help make the final decision:

How sure do I want to be that this data is gone?

As the world continues to evolve technologically, so do cybercriminals, and discarded data is no exception on the list of targeted information. The sensitivity of the stored data and the consequences that would result from a breach of said information

should be the first question and most critical consideration when deciding between in-house or third party data destruction. Regardless of volume or budget, if the information is sensitive and therefore protected by regulatory requirements, organizations should seriously consider implementing in-house destruction. With the density of data stored digitally, even just one hard drive falling into the wrong hands can have catastrophic consequences.

What is the volume of data I have to destroy?

The volume of media to be destroyed at a location will influence almost every other decision to be made going forward within the policy. Data destruction devices are available in various sizes and with a variety of differences including throughput, physical size, and power consumption. Similarly, ITADs have different plans that correspond with the amount of data being destroyed, including a drive-by-drive price option or a bulk price for multiple drives.

What is my budget?

In a perfect world, budget should be the last consideration, but it ultimately is the basis for nearly every decision. ITADs are almost certainly the cheaper option in the short term, but a location that regularly has data to destroy would find an in-house data destruction machine pays for itself fairly quickly. In the long term, ITADs will become very costly with repeated orders and trips, while in-house machines require maintenance in order to maintain efficiency and longevity.

Another budgetary item to consider is cost of breach. There is a popular meme in the cybersecurity world of social media that shows a cybersecurity budget before breach as being pennies, while after a breach it is a windfall of dollars (at right). Unfortunately, this is a reality many smaller businesses never experience, since 60% of small businesses who suffer a breach are out of business within six months. Data breaches are costly in terms of regulatory fines, remediation fees, and lost revenue due

to eroded customer loyalty. The time to consider a cybersecurity budget is BEFORE a breach occurs. Purchasing fire insurance after your home burns down is too little too late, and the same can be said for protecting sensitive data.

Each Policy is Made Uniquely

Drafting a data decommissioning policy is no easy task. With so many variables and moving parts, it is imperative to read, educate, and determine the main focus of an organization's policy for destroying data. Does the data need to be destroyed as securely as possible? As inexpensively as possible? As quickly as possible? A policy can be custom tailored to accommodate an organization's specific requirements, but ultimately the most critical aspect of finding the right solution is meeting the required compliances and regulations for a particular organization.

And education shouldn't stop with the policy writer, or even stop once the policy has been drafted. All personnel that come into contact with sensitive data should also be educated on the risks and proper procedures for handling, storing, and destroying sensitive data and preventing leaks, as well as the effects a breach can have on an individual and to an organization as a whole. The strictest policy and requirements will mean nothing if the people implementing and enacting the decommissioning policy have a disregard for security, and it is important to state such during continued training and education.

So what solution is best? Whether destroying data in-house or through the use of a third-party, organizations will need to decide on a case-by-case basis. No two policies will be drafted the same, but by following industry regulations and performing due diligence, organizations that draft, implement, and continuously educate employees on a policy will be far more secure than those who do not.

Security Engineered Machinery Co., Inc.
5 Walkup Drive | Westboro, MA 01581
800.225.9293 | 508.366.1488
contact@semshred.com
www.semshred.com