SEM®

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

MEDIA SANITIZATION

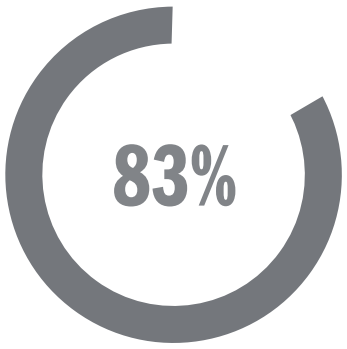
BEST PRACTICES FOR ORGANIZATIONS

IT TAKES 20 YEARS TO BUILD A REPUTATION AND A FEW MINUTES OF CYBER-INCIDENT TO RUIN IT.

– STĒPHANE NAPPO

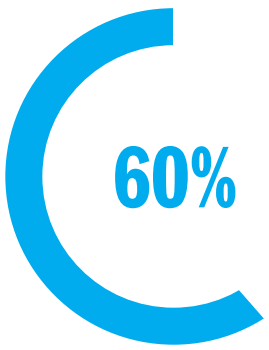
CYBERSECURITY STATS

IBM Security and Ponemon Institutes' The Cost of a Data Breach Report offers IT, risk management and security leaders a lens into factors that can increase or help mitigate the rising cost of data breaches. This research studied 550 organizations impacted by data breaches. The breaches occurred across 17 countries and regions and in 17 different industries. Key stats:



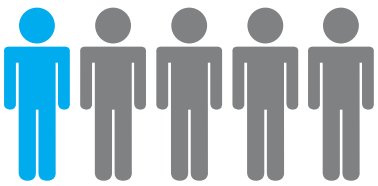
RISK IS EVERYWHERE

83% of organizations studied have had more than one data breach.



BREACHES AND LEAKS ARE EXPENSIVE

60% of organizations' breaches led to increases in prices passed on to customers.



THIRD-PARTY RISK IS REAL

One in five breaches occurred because of a compromise at a business partner.

REACHING AN ALL-TIME HIGH, THE COST OF A DATA BREACH AVERAGED USD 4.35 MILLION IN 2022. THE UNITED STATES HAD THE HIGHEST AVERAGE TOTAL COST OF A DATA BREACH AT USD 9.44 MILLION.

DETERMINING RISK

IS THERE A STATUTE OF LIMITATIONS ON BREACH FROM END-OF-LIFE MEDIA?

NO. It is really that simple. If a discarded or recycled drive or device is involved in a breach 5, 10, or 20 years down the road, the originating organization is still responsible. Because so many drives and devices end up in highly targeted and highly pilferable landfills and trash heaps, this lack of a statute of limitations is concerning.

End-of-life data destruction isn't just good sense for the present; it also makes sense for the future.

As technology evolves, so do ways in which cybercriminals and nefarious organizations or individuals can access data. Organizations typically prioritize active and resting data security protocols such as firewalls, threat detection, etc., but pay little attention to end-of-life data — a risky practice. Media sanitization should also be prioritized, and the cost to do so is comparitively minimal.

SECURITY STANDARDS

DIN 66399 – The International Standard

DIN 66399 standards are internationally recognized; however, DIN standards are subjective in nature, with the organization housing the data being sole determiner of the data's security level, of which there are three protection classes:

- Class 1 is for the normal protection required for internal data where disclosure would have a negative impact on a company or a risk of identity theft of an Individual
- Class 2 is for the higher protection for confidential data where disclosure would have a considerably negative effect or could breach legal obligations of a company, or offer a risk of adverse social or financial standing of an individual
- Class 3 Is for very high protection for confidential and top secret data which, if disclosed, could have terminal consequences for a company or government entity, and have a health and safety or personal freedom risk to individuals

DIN 66399 covers six types of media: Paper (P), Film (F). Magnetic, which includes data tape and diskettes (T), Hard Drives (H), e-Media, such as thumb drives and solid state media (E), and Optical, which includes CDs, DVDs, and Blu-ray Disks (O). Under each of these designations are seven security levels. For classified media, for example, paper must be destroyed to level P-7, which requires a final particle size no larger than 1mm x 5mm (shown below). For less sensitive data, a P-4 particle will suffice.

A comprehensive introduction to DIN 66399 may be found on our website at www.semshred.com/DIN66399.

NIST 800-88 – The US Standard

In the United States, NIST 800-88 is is the most accepted standard for end-of-life media sanitization, including for FedRAMP. The basic three media sanitization methodologies are Clear, Purge, and Destroy. Knowing when to use which methodology for IT media depends on the sensitivity of the data and the organization's IT security professionals' recommendation.

FedRAMP™

The Federal Risk and Authorization Management Program (FedRAMP®) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government, with an emphasis on security and protection of federal information. FedRAMP references NIST 800-88 with regard to media sanitization.

Clear
Clear uses overwriting with basic read/write commands. Note that basic read/write overwriting is never recommended as it does not address all blocks on the media. Drawbacks to overwriting are many: 1) it is only effective for magnetic media, not solid state or flash; 2) this methodology is wide open to operator error and theft; and 3) undetected failure is quite common, leaving large swaths of data fully recoverable.

Purge
Purge uses state-of-the-art overwrite, block erase, and cryptographic erase methodologies that makes data recovery for the most part infeasible. It provides a higher level of media sanitization than Clear and is therefore utilized when sanitizing more sensitive data. The benefit to purging is that the media is reusable. The drawbacks are many: 1) no purge methodology is foolproof; 2) purge methodologies are highly prone to human error; 3) purging is extremely time-consuming and can take days (!) for one large drive.

Destroy
While clearing and purging provide adequate media sanitization involving less sensitive data, destroying is the most effective and permanent solution for secure data applications. Destruction includes electromagnetic degaussing, as well as physical destruction by crushing, shredding, or disintegrating. The one drawback to the Destroy methodology is that the media cannot be reused. That said, the benefits far outweigh this one drawback: 1) destruction takes seconds to accomplish; 2) data is fully unrecoverable; and 3) there is no room for human error when a hard drive is reduced to tiny pieces.

NSA/CSS – The US Intelligence Community Standard

For classified and top secret information, the National Security Agency (NSA) and Central Security Service (CSS) determine the appropriate data destruction methodology and evaluates equipment for this purpose. The NSA's requirements for end-of-life media sanitization ensure that any and all data will be absolutely unrecoverable, even if subjected to sophisticated data recovery techniques.

NSA/CSS Policy Statement 9-12 "NSA/CSS Storage Device Sanitization" provides guidance for sanitization of information on storage devices for disposal. Unlike most other data disposal policies, NSA/CSS Policy Manual 9-12 provides clear and precise requirements on secure disposal and destruction of data bearing media. NSA/CSS Policy Manual 9-12 also provides information on how to obtain NSA/CSS Evaluated Products Lists (EPLs) that meet NSA/CSS specifications. While this may seem extreme to commercial organizations, the fact remains that all other end-of-life security protocols are subjective and open-ended.

NSA/CSS Standards

HDDs AND MAGNETIC MEDIA

Rotational hard disk drives and magnetic media such as floppy disks and data tapes must follow a two-step process: degauss in an NSA listed degausser, then physically destroy using an NSA listed crusher or any shredder.

SSDs and eMEDIA

As they cannot be degaussed, SSDs and eMedia must be physically destroyed to a 2mm particle.

OPTICAL MEDIA

CDs must be destroyed to a 5mm particle. Because they are denser, DVDs and Blu-ray Discs (BDs) must be destroyed to a 2mm particle.

PAPER

Paper must be destroyed to a 1mm x 5mm maximum particle size. NIST 800-88 and DIN 66399 P-7 also follow this protocol.

NSA/CSS LISTED MEDIA SANITIZATION EQUIPMENT

It's All About the Evaluted Products Lists (EPLs)

NSA evaluated equipment is just that: devices that have been rigorously tested and approved by the NSA to meet their stringent security requirements for destruction of end-of-life media. This testing includes determination that the final particle produced is consistent with the NSA's requirement. The NSA's evaluation also includes a 1-hour durability test that ensures the device can run and meet the mandated particle size for a solid hour without jamming or overheating.

The NSA maintains a list of evaluated equipment for each type of media requiring end-of-life sanitization. These lists can be found on the NSA's website and are updated frequently. Scan the QR code for up-to-date lists.

< NSA Evaluated Products Lists

Not Just Government

Cloud service providers, data centers, colos, and other commercial security-centric organizations also follow NSA standards for end-of-life media sanitization.

In fact, the Australian government also follows NSA standards for its own government data. The NSA has long set the precedent for best practices in media sanitization.

FINANCIAL AND PROFESSIONAL SERVICES

While some industries are not subjected to any end-of-life data security regulations, financial services organizations are subjected to many.

GLBA and the Safeguards Rule
Covered Entities: Non-Bank Financial Institutions
Governed by the Federal Trade Commission (FTC)

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is a United States federal law requiring financial institutions to explain how they share and protect their customers' private and nonpublic personal information (NPI). Covered entities must develop, implement, and maintain a comprehensive information security program that includes physical safeguards appropriate to defining attributes of the affected organization and the sensitivity of the NPI at issue.

In 2021, in direct response to widespread and devastating data breaches, the Federal Trade Commission enacted an updated rule under GLBA that strengthens data security safeguards (the "Safeguards Rule") that financial institutions must implement to protect their customers' financial information. The Safeguards Rule applies to all non-bank financial institutions, even loosely identified as such, including mortgage companies, pawn brokers, and car dealers.

A key aspect of the Safeguards Rule requires that non-bank financial institutions implement a policy for the secure disposal of customer information no later than two years after the last date that the information was used, unless retention is otherwise required for legal, regulatory, or legitimate business purposes.

While the Safeguards Rule under GLBA requires data disposal after two years of non-use, it does not mandate a specific data destruction methodology. Best practice for complying with the 2021 Safeguards Rule includes following NIST 800-88 data disposal requirements.

Sarbanes-Oxley (SOX)
Covered Entities: Corporate Financial Organizations
Governed by the Securities and Exchange Commission (SEC)

Passed in 2002 because of numerous large accounting scandals, the Sarbanes-Oxley Act (SOX) is a law enacted by the Securities and Exchange Commission that sets forth standards for recording and reporting of corporate financial activities. Prior to Sarbanes-Oxley, there was little government oversight and virtually no possibility of criminal prosecution for the board members of publicly traded companies, some of whom therefore fraudulently misrepresented their books and earnings, causing catastrophic financial damage to millions of investors. Remember Bernie Madoff?

A key part of Sarbanes-Oxley involves record retention. To maintain SOX compliance, businesses must retain their records for a set period of time. Covered records include any documents with financial or sensitive client information including financial statements; accounting records; sales reports; emails; memos; instant messages; bank statements; and invoices, to name a few.

While there is no set regulation for the disposal of covered records, SOX makes it clear that records must be meticulously and accurately maintained without alteration. Since it is not possible to keep all records indefinitely (and in some cases is illegal, depending on whether this private information is covered by another data security regulation), organizations that fall under SOX should dispose of records upon expiration using, at a minimum, NIST 800-88 data disposal requirements.

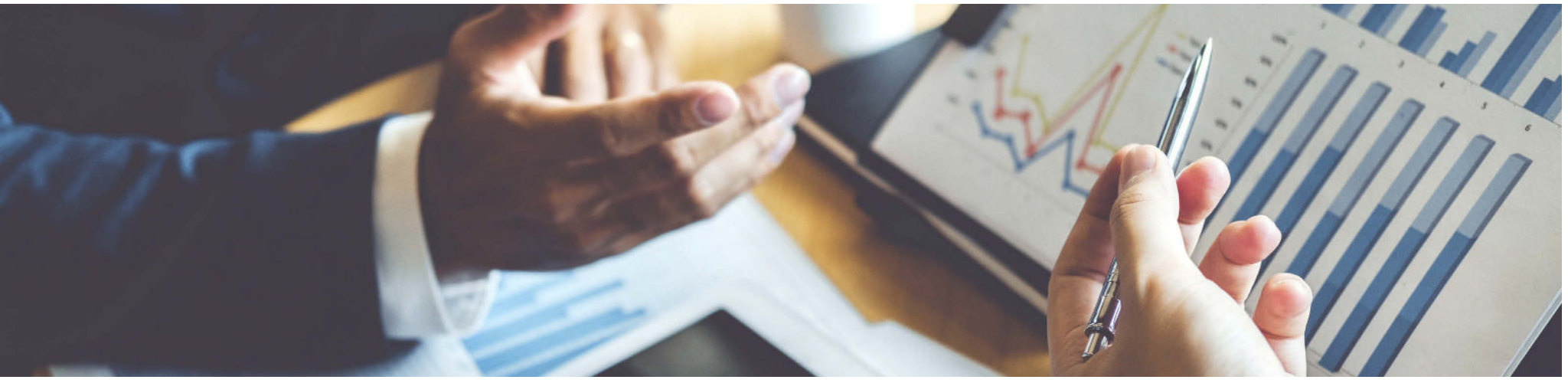
FACTA
Covered Entities: Organizations Utilizing Consumer Reports Governed by the Federal Trade Commission (FTC)

An addendum to the Federal Trade Commission's Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transactions Act of 2003 (FACTA) Disposal Rule went into effect in 2005 and requires businesses and individuals to appropriately dispose of sensitive consumer reports. Organizations and individuals who use consumer reports for any business purpose are subject to the requirements of the Disposal Rule, which calls for consumer reports disposal to protect against "unauthorized access to or use of the information."

It is important to note that there is no standard for the proper disposal of information derived from a consumer report and that it is instead flexible, allowing organizations covered by the Rule to determine disposal methodology based on the sensitivity of the information and costs associated with the disposal of such information.

The Rule applies to individuals and organizations of all sizes that use consumer reports, including but not limited to consumer reporting companies; lenders; insurers; employers; landlords; government agencies; mortgage brokers, car dealers; attorneys; private investigators; debt collectors; individuals who pull consumer reports on prospective home employees, such as nannies or contractors; and entities that maintain information in consumer reports as part of their role as a service provider to other organizations covered by the Rule.

As there are no specific disposal requirements with FACTA, NIST 800-88 data disposal methodology should be followed.



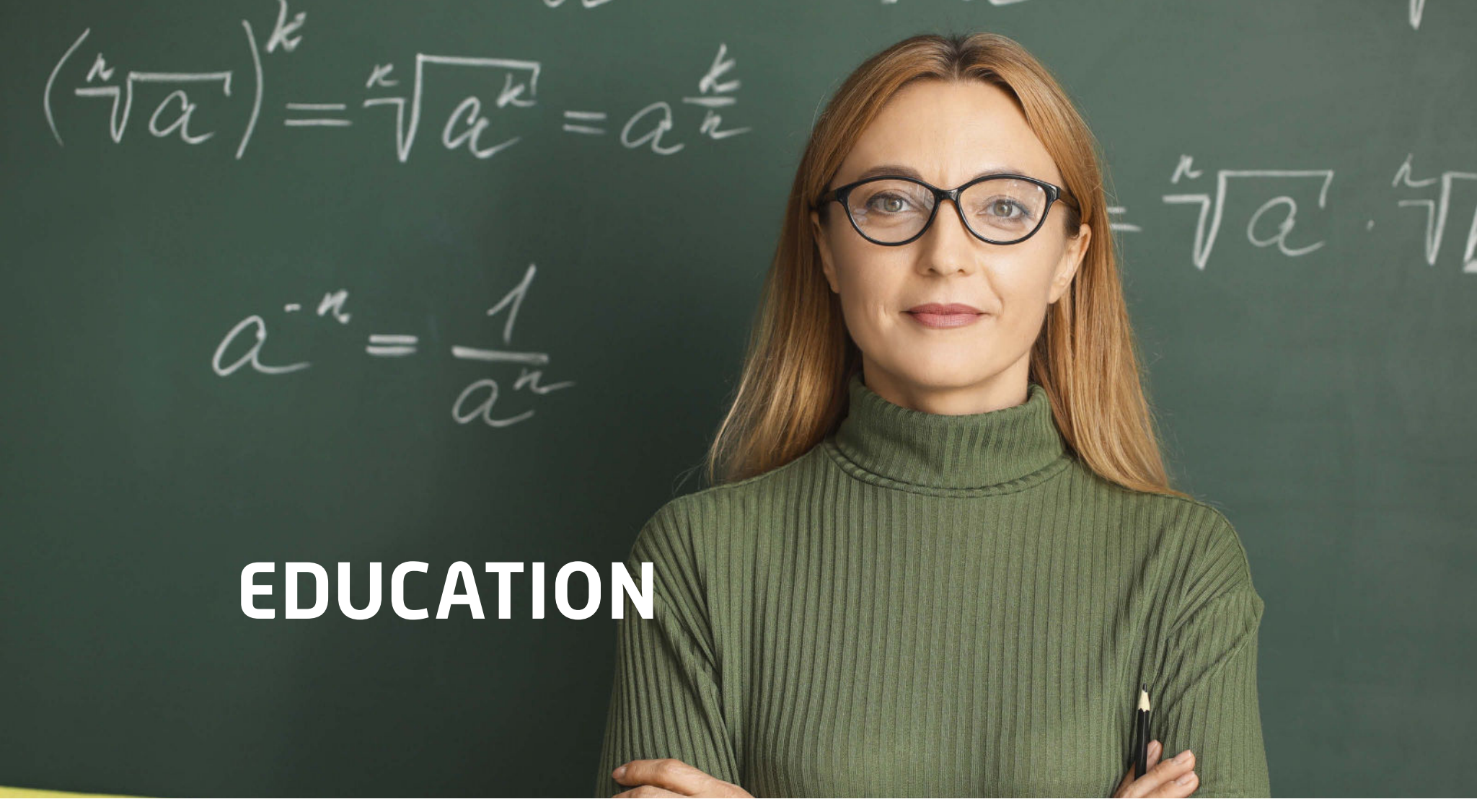
HIPAA
Covered Entities: Health Organizations
Governed by the U.S. Department of Health and Human Services

The Health Insurance Portability Accountability Act (HIPAA) was enacted in 1996 by the U.S. Department of Health and Human Services to require covered entities to safeguard the privacy of protected health information (PHI) in any form. This means that organizations must implement procedures that limit incidental — while fully avoiding prohibited — uses and disclosures of PHI including disposal. HIPAA requires that covered entities to implement procedures to specifically address disposition of electronic PHI as well as the hardware or e-media on which it is stored.

In laymen's terms, this means that covered entities are never permitted to dispose of any PHI or the media on which it is housed in dumpsters or other publicly accessible containers, nor is PHI allowed to be simply abandoned. That said, like most other data security regulations, HIPAA does not mandate a specific disposal methodology but rather references NIST 800-88 while asking organizations to determine their own disposal policies. Typically, organizations determine their own circumstances and potential risks to determine the most appropriate methodology to safeguard PHI and the required steps to do so. PHI such as name, social security number, credit card number, diagnosis, treatment information, or other sensitive information require more stringent care due to the risk of identity theft or harm to a person's reputation. This data may be stored on paper, e.g. as when patients fill out their own information in doctor's offices, or may be stored digitally, such as on hard drives or removable storage media.

Those who must comply with HIPAA include but are not limited to the following: health insurance companies; HMOs, or health maintenance organizations; doctors; clinics; psychologists; dentists; chiropractors; nursing homes; and pharmacies.

As there are no specific disposal regulations with HIPAA, NIST 800-88 data disposal methodology should be followed.



EDUCATION

FERPA
Covered Entities: Public Educational Institutions
Governed by the U.S. Department of Education

The Family Educational Rights and Privacy Act of 1974 (FERPA) protects the privacy of sensitive and personally identifiable information (PII) in student education records and applies to all educational institutions that are the recipients of federal funding. FERPA prohibits the disclosure of student or parent information including health and immunization records; transcripts; disciplinary action; and student and parent PII such as name, address, telephone, and social security number unless given consent by the student (if over the age of 18) or the parent, or for reasons expressly required by the institution. In addition, the institution is required to document any disclosure of PII under FERPA.

While a specific disposal requirement is not mandated under FERPA, improper disposal of student records may result in non-compliance in two ways: 1) by disclosing PII without consent and 2) failing to document said disclosure. The federal government may penalize educational institutions found to be in non-compliance with FERPA by withholding further payments under applicable programs or even terminating eligibility to receive funding.

Best practice for FERPA compliance includes following NIST 800-88 data disposal requirements. All of SEM's high security paper shredders, disintegrators, IT shredders, IT crushers, and degaussers are appropriate for the disposal of student records covered data following NIST 800-88 protocols.

CONSUMER CREDIT AND SECURITY PRINTERS

PCI DSS
Covered Entities: Organizations that Process, Store, or Transfer Consumer Credit Card Information
Governed by PCI SSC

Governed by the Payment Card Industry Security Standards Council (PCI SSC), the Payment Card Industry Data Security Standard (PCI DSS) was formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International, and American Express in an effort to secure credit and debit card transactions against fraud and theft. PCI DSS compliance requires covered entities to protect customer credit card data including personally identifiable information (PII), credit and debit card numbers and CVV, and other sensitive information used in the processing and transfer of payment cards. As part of PCI DSS, PCI Requirement 3.1 mandates that organizations securely dispose of data that is not otherwise legally required to be maintained.

PCI DSS covers organizations that process, store, or transmit payment card data, including any company or store that sells good or services and processes credit cards; service providers who process credit card details and data as part of their service or product, such as payment processors or ATM machine manufacturers; banks who house and process credit and debit card information; and secure printers who print debit and credit cards.

While PCI DSS requires that cardholder data must be destroyed unless legally mandated otherwise, it does not mandate a specific data destruction methodology. That said, the penalties for non-compliance with PCI DSS's data disposal requirements are severe. As such, covered entities should have a clear policy to dispose of any and all data no longer needed, including both hardcopy information as well as electronic media such as hard drives, removable storage, servers, and any other forms of recordable media.

Best practice for PCI Requirement 3.1 compliance includes following NIST 800-88 data disposal requirements.

SECURITY STANDARDS: DATA CENTERS

When it comes to data centers, the number of security regulations to which they must adhere is staggering. Because data centers carry data from so many different types of organizations, they must follow a myriad of regulations covering numerous types of data:

Educational:
The Family Educational Rights and Privacy Act (FERPA), the Higher Education Opportunity Act (HEOA), the Protection of Pupil Rights Amendment (PPRA), and, for European students, the General Data Protection Regulation (GDPR).

Healthcare:
The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

Financial:
The Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI DSS).

Research:
The Federal Information Security Modernization Act (FISMA) and the National Institute of Standards and Technology (NIST) Special Publication 800-171.

Government:
NIST 800-88 and NSA/CSS Media Sanitization.

Trying to meet the demands of 10+ different security regulations is nearly impossible. The simplest and most cost-effective way to determine appropriate sanitization is to follow NSA/CSS for classified and top secret, and NIST 800-88 for everything else.

ALL DATA LEADS TO DATA CENTERS

It's Really That Simple

Over the last few pages, we talked about data security regulations and how to comply. However, the fact remains that nearly everything now resides in data centers. X-rays from hospitals? In the cloud aka data centers. Professional services files? Stored in DropBox or OneDrive or iCloud or any other cloud service aka data center. Student and employee files? You guessed it: data centers. So while learning about mandates that regulate each industry is important, at the end of the day, it all comes down to data centers.

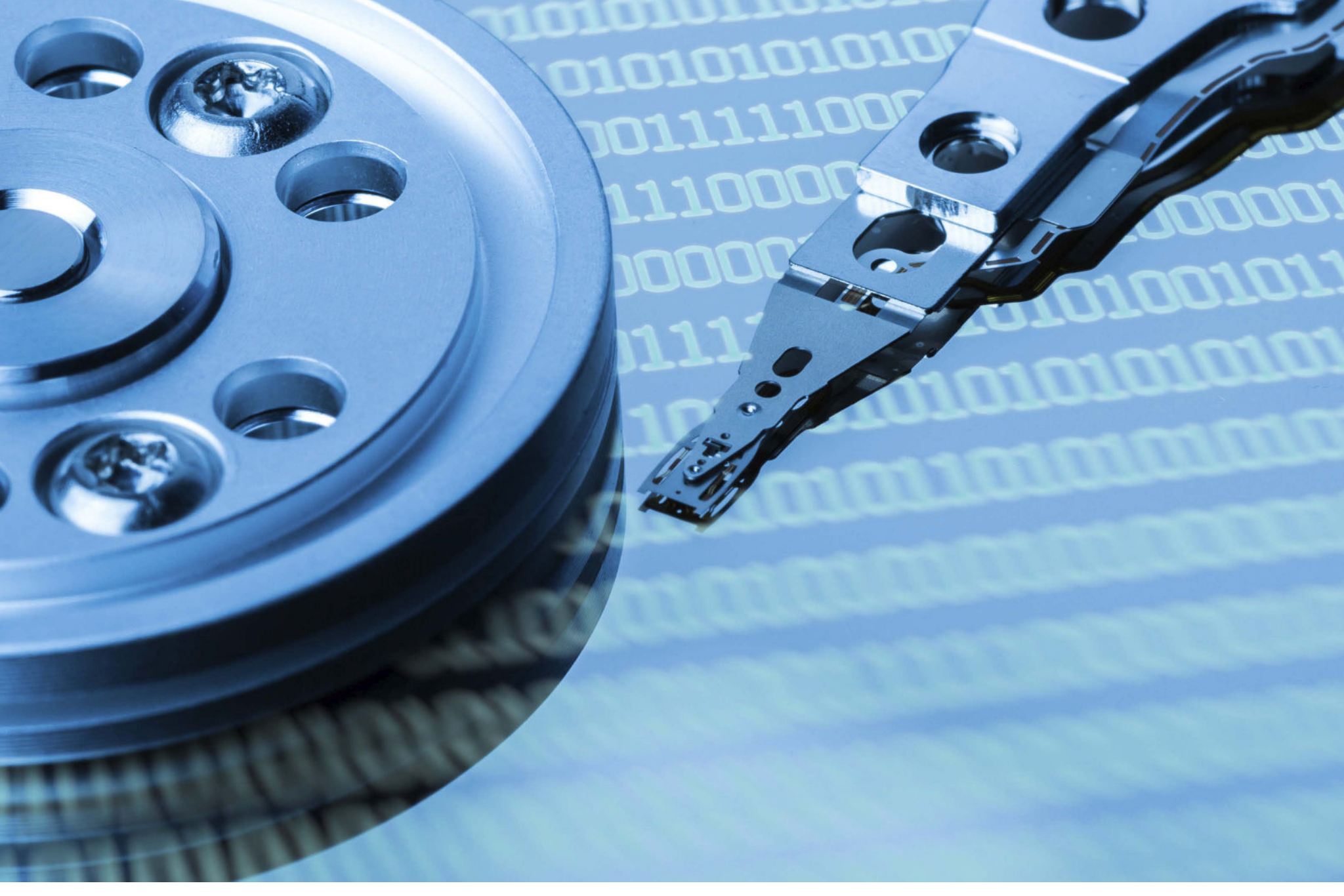
The good news is that every single security regulation previously discussed, aside from US classified and top secret, can be met by following NIST 800-88 protocols. It really is that easy.

Data centers can rest easy if they follow NIST 800-88 protocols for unclassified information and NSA/CSS for classified. And SEM has the equipment to help: whether NIST 800-88 or NSA/CSS, SEM has the data destruction equipment to meet all data center requirements..

NIST 800-88 and NSA/CSS

Confused about how to meet the myriad regulatory requirements for differing industries? It all comes down to two standards: NSA/CSS for classified and top secret, and NIST 800-88 for everything else, even FedRAMP and CUI.

CONTROLLED UNCLASSIFIED INFORMATION



WHAT'S MY MEDIA?

Now that you know how to destroy media to security standard specifications, we want to make sure you know what type of media falls into which category.

There are six basic media categories that encompass all types of data-bearing media. Since there are so many different types of material that can contain high security, sensitive, or personally identifiable information (PII), figuring out which category your media falls into can be a challenge.

On the next page, we've broken down each category into its major components. This can be useful for determining which destruction mandate and associated device should be used for end-of-life data destruction.

MEDIA TYPES

Media is typically broken down into six major categories, which cover nearly all data-bearing devices at this time.

PAPER

Printed non-digital media, such as paper, printing plates, and tipping foil

FILM

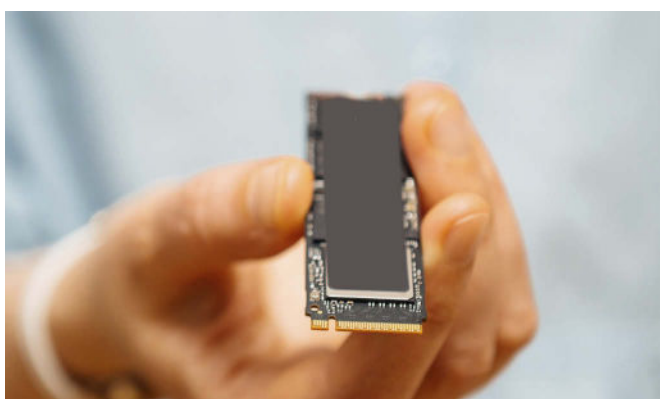
Micro-film, microfiche, slides, x-rays, and other film products

MAGNETIC

Floppy discs, key cards, ID cards, magnetic tapes, credit cards

ROTATIONAL

Hard drives from computers, laptops, external devices, and data centers



E-MEDIA/SSD

Solid state drives, memory sticks, thumb drives, mobile phones, tablets

OPTICAL

CDs. DVDs, and Blu-ray Discs (BDs)

DESTRUCTION TYPES

The protection of end-of-life information is far simpler than protection of active data. While active data requires firewalls, security protocols, encryption, and a myriad of other highly technical — and expensive — methodologies, protecting end-of-life data is relatively simple: destroy the data.

01 DEGAUSSING

Degaussing is a process that creates powerful magnetic fields to sanitize magnetic storage media, rendering the drive useless. Degaussable media includes rotational hard drives; computer, audio, and video tapes; and magnetic removable storage media such as floppy, ZIP, JAZZ, REV, and Syquest disks.

02 CRUSHING

Crushing is the act of deforming a drive or device to make it unusable. The most common type of crusher uses a conical punch to pierce rotational hard drives. Additionally, SEM has created proprietary SSD crushers that utilize toothed rotors to pierce and crush even the tiniest microchips.

03 SHREDDING

Shredders incorporate toothed cutting blades that tear media to a specific particle size. High security paper shredders cross-cut to 2mm, while HDD shredders tear hard drives to a 38mm particle. Shredding is appropriate for paper, hard drives, optical media, film, license plates, and credit cards, to name a few.

04 DISINTEGRATING

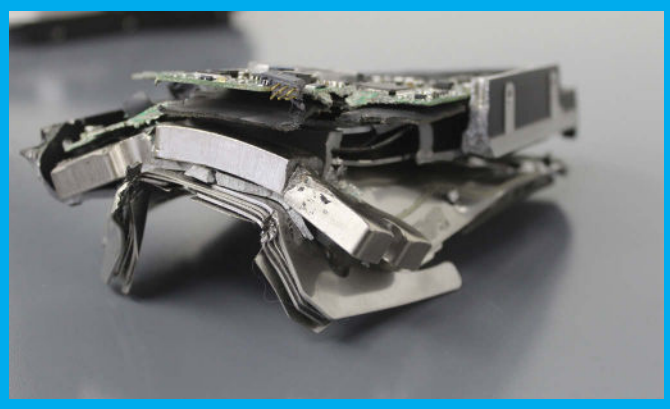
Disintegrators utilize stationary and rotating blades that continuously cut material to a size small enough to fit through a screen that is determined by the media being destroyed. Disintegrators destroying classified and high security solid state drives or paper are equipped with a 2mm screen, while those destroying less sensitive data may use a larger screen.

EXAMPLES

BELOW ARE SOME VISUAL SAMPLES OF SHRED SIZES FOR EACH OF THE TYPES OF DESTRUCTION:

DEGAUSS

While degaussing sanitizes all data on a drive, there is no visual confirmation. For this reason, the NSA requires classified drives to be physically destroyed after degaussing. Security-centric commercial organizations also follow this best practice.



CRUSH

Shown is a hard drive (HDD) crushed in an SEM 0101 hard drive crusher. The 0101 is capable of crushing all types of hard drives including enterprise drives, glass drives, laptop drives, server drives, and data center drives.

SHRED

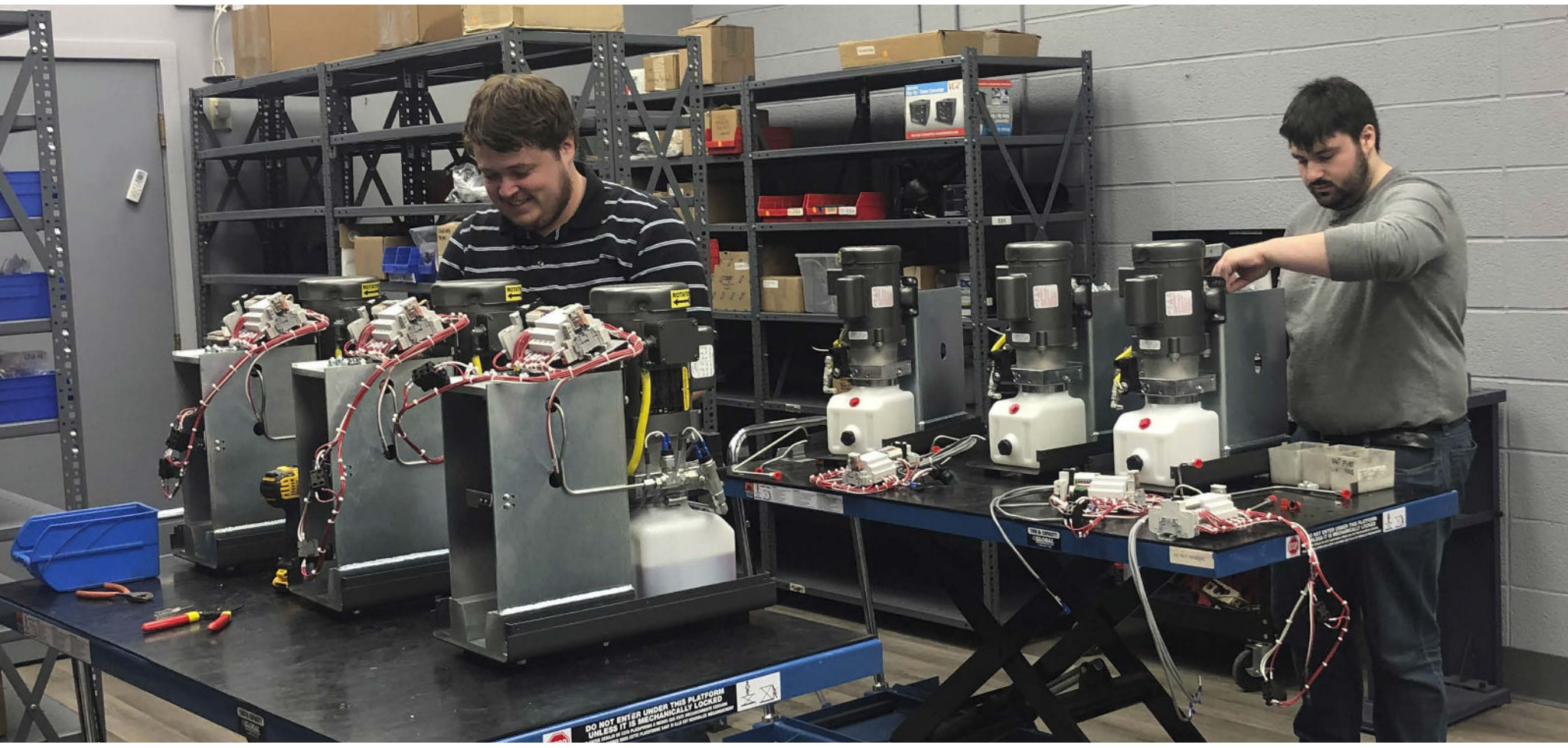
Shown is a hard drive shredded in an SEM 0305 hard drive shredder. Shredders are capable of shredding rotational hard drives and solid state drives, and are available as combo machines to destroy both HDDs and SSDs in one device.

DISINTEGRATE

Pictured is a solid state drive disintegrated in the NSA listed SEM SSD2-HS solid state disintegrator. The final particle size is 2mm, the NSA mandate for classified solid state media. Disintegration is overkill for most commercial organizations.

WHO WE ARE

IN BUSINESS FOR OVER 50 YEARS, SEM'S SOLE PRODUCT LINE IS HIGH SECURITY INFORMATION DESTRUCTION EQUIPMENT AND OUR TARGETED AREA OF EXPERTISE IS INFORMATION END-OF-LIFE SECURITY.



Established in 1967, SEM is proud to be a US manufacturer that provides comprehensive end-of-life solutions for the protection of sensitive information in government and commercial markets. SEM data destruction devices are the premier high security choice available on the market today.

Whether paper, hard disk or solid state drives, tape, microchips, or any other type of media-bearing device, SEM has a solution that can sanitize classified and top secret information as well as controlled unclassified information (CUI), personally identifiable information (PII), personal health information (PHI), or any other type of sensitive data. SEM also produces customized equipment for size reduction solutions and for destroying off-spec or returned product for the medical device, gaming, security printing, and food industries as well as bank note/currency destruction for the US Federal Reserve and Central Banks throughout the world.

CONTACT US

5 Walkup Drive | Westborough, MA 01581

Phone: 508-366-1488
e-mail: contact@semshred.com

www.semshred.com

SEM®

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