Media Sanitization Guide

Tom Olzak CISSP
November 2019

Introduction

Protecting sensitive information requires attending to where the information is located and used throughout its lifetime. This document guides how to manage sensitive information when the media on which it resides is no longer used for that purpose. These management processes are collectively known as media sanitization.

Media comes in several forms: magnetic, paper, solid-state, and optical. I address sanitization across all of these media types, including how to meet associated data erasure challenges. Further, this guide provides steps and considerations needed to implement and manage media sanitization policies and procedures.

Sanitization and Data Remanence

Media sanitization uses reasonable and appropriate tools and techniques to make the recovery of stored data too challenging to be of value to data thieves. The value of the data varies according to theft motivations and the financial return vs. data recovery effort.

For example, customer information that includes payment card information is sensitive information with inherent value to data thieves. However, a thief is only going to go after the data if the time and effort required results in a cost lower than the value of the data. Consequently, a simple overwrite of a magnetic disk is likely enough to prevent attempts to recover the information.

Risk

Sanitization approaches implemented by organizations must match the risk associated with the stored data. Figure 1 shows one way to look at how we manage this risk. By increasing the skills and tools (means) and the opportunity (availability of retrievable data) needed to recover the data, we reduce the likelihood that an attacker can locate and retrieve sensitive data from repurposed or retired media (Olzak, 2012).

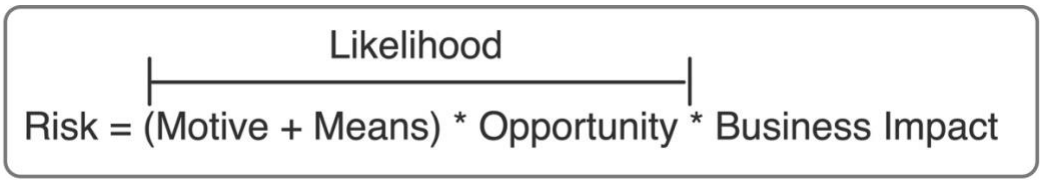

Figure 1 Risk Formula

Another essential element of likelihood is the value of the data to the attacker (motive). Motive often goes beyond data value. Hacktivists might want to steal data to embarrass or harass a target organization. Nation-state hackers seeking to steal defense secrets from other nations are highly motivated… and the cost is not usually an issue.

The final element of risk, not shown in Figure 1, involves regulatory requirements. Regulations like the HIPAA require proper disposal of media. Risk management is a large part of sanitization planning, as described later in this guide.

Go to Table of Contents

Data Remanence

Data remanence is residual data remaining after an organization takes steps to delete it. For magnetic and solid-state (SSD) drives, deleting files and databases is not enough. When a person deletes a file, for example, the information in the file is not deleted. Instead, the file system marks the locations where the file is stored as no longer used. Usual methods for accessing the file via the operating system no longer work. However, anyone can easily download one of the many tools that can read "deleted" files. Data remains on the drive until other information is written over it.

File systems that implement journaling, including Microsoft's NTFS, write data to logs and files to safeguard integrity (LSoft Technologies Inc., 2019). This can result in sensitive information remaining in journaling logs. Consequently, solutions like file shredding might not completely remove all related sensitive information from a disk.

Areas on disks not currently mapped for use (e.g., marked as defective) are often skipped during simple overwrite processes (Kissel, Regenscheid, Scholl, & Stine, 2014), and defragmentation processes write file data to various locations. Both conditions can make sanitization with simple overwrites difficult.

Go to Table of Contents

Sanitization Levels

The National Institute for Standards and Technology (NIST) provides detailed sanitization guidance in SP 800-88 r1. In this document, the NIST describes three levels of sanitization: clear, purge, and destroy.

- **Clear** is a simple overwrite of the media with meaningless data. Sanitization tools commonly do this by writing all zeros to user-accessible areas. This does not address areas of possible remanence I described earlier.
- **Purge** completely destroys all data on media. It goes beyond simple overwrites and includes cryptographic erase and degaussing.
- **Destruction** involves reducing the media to small pieces or ash.

I describe purging and destruction approaches across all media types later in this guide.

Figure 2 (Kissel, Regenscheid, Scholl, & Stine, 2014, p. 17) shows a general decision flow chart for deciding which sanitization approach to use. These are guidelines. Sanitization risk assessments related to an organization's unique operating environment are still needed.

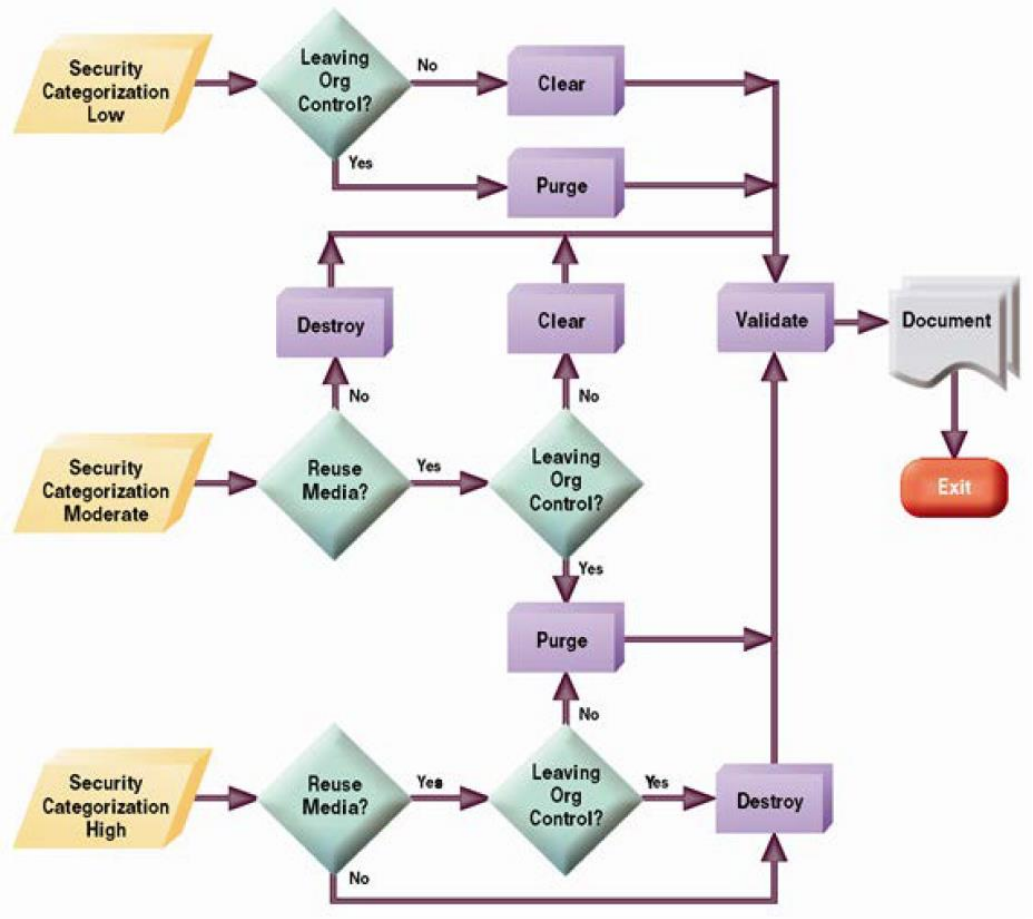

Figure 2 Sanitization Decision Flow Chart

Note that the foundation of the flow chart is data categorization (classification). For the rest of this guide, Figure 3 translates the NIST categories with the more common classifications, as described in the linked document.

Categorization	Classification
Low	Public
Moderate	Confidential
High	Restricted

Figure 3 Categorization vs. Classification

Go to Table of Contents

Sanitization Procedures by Media Type

Although overwrite, purge and destruction are commonly accepted sanitization procedures, organizations cannot use all three across all media types. It is important to understand what is effective for each type.

Magnetic Drives

Clear

Magnetic and SSDs can be cleared, purged, or destroyed. Many tools exist to allow simple overwrites of entire user-accessible disk areas. However, organizations should not use overwrites on SSDs if they plan to reuse them. Because of the way SSDs manage wear levels, overwrite can severely limit an SSDs lifetime if done multiple times.

Windows and macOS come with overwrite capabilities. Other products include those listed in a Techworld article (Best disk wiping tools for hard drives, smartphones, and SSDs, 2018). Keep this list available. These tools (free and for-fee) include both clear and purge capabilities.

Purge

Clearing is not enough if

- The data is confidential, and the drive is leaving the organization
- The data is restricted

Purging is needed when media with restricted data is reused within the organization or when media classified as confidential or higher leaves the organization for reuse or disposal.

Secure Erase

Today's PATA and SATA drives usually come with Secure Erase commands that effectively purge them of data (Fisher, 2019). Secure Erase, a drive standard not available for SCSI drives, writes a binary one or zero across all areas of the disk: not just those that are accessible during normal drive operation. It is done on the drive itself using utilities that come with the drive. For SCSI drives, third-party software is often necessary.

Cryptographic erase with SED

Cryptographic erase (CE) can be the most reliable approach to purging data. If encryption is implemented *before* sensitive data is written to the disk, and it is demonstratable that keys can be securely erased, no data in any disk location is available to attackers. Two approaches to CE include self-encrypting drives (SEDs) and the use of encryption capabilities in operating systems.

Figure 4 (Buecker, 2015) helps us understand how CE works. The media encryption key (MEK) is stored in a special location on the drive. It is used to encrypt all content written to the drive with the Advanced Encryption Standard (AES). The MEK is encrypted with a key encryption key (KEK) using an encryption processor on the drive. The KEK is not stored on the drive, and it is provided to decrypt the KEK at system powerup. For example, when a user logs onto a device with an SED, the KEK decrypts the MEK allowing user and system access to the drive content.

When purging the drive, a special utility provided by the drive manufacturer is used to change the MEK to one that has no relationship to the encrypted data. It cannot be used to decrypt the drive content. This effectively makes data on the drive inaccessible.

SEDs are often not widely distributed in organizations. Because the cost of SEDs is higher than that for standard drives, systems that contain them cost more. Many vendors do not include SEDs in general system configurations because of this cost. Organizations have to ask to have SEDs in any vendor proposal for system pricing.

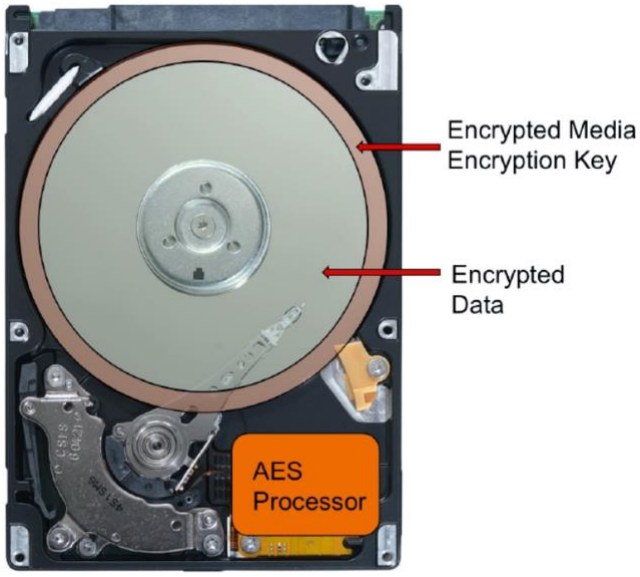

Figure 4 SED

Cryptographic erase with operating systems

Lack of SEDs does not mean CE is not possible. Both Microsoft Windows and Apple macOS provide the means to encrypt drives and finally perform CE. However, these approaches can take longer than a simple key removal.

Windows. BitLocker comes with Windows Vista (and later) Pro, Enterprise, and Server 2008 (and later). It can encrypt both internal and external drives. A reliable approach to CE involves these steps for a drive already encrypted with BitLocker:

1. Use the Windows Disk Manager utility to delete the encrypted volume
2. Create a new volume using the same disk space as the deleted volume
3. Use BitLocker to encrypt the new volume using a different passcode/key

This is a very quick process. Step 3 is performed on what the Disk Utility sees as empty disk space, so encryption is very fast.

If the drive or volume is not already encrypted, an organization can first encrypt the drive and then follow the three purge steps.

Go to Table of Contents

macOS. FileVault, the encryption capability that ships with macOS, enables both cryptographic erase and a complete overwrite of data, as shown in Figure 5. Using the *Disk Utility*, select the disk to be erased and click *Erase*. After clicking *Security Options* at the lower left, move the slider all the way to the right. All data on the drive is made inaccessible. If the drive is encrypted with FileVault, this process removes all keys.

Moving the slider to the right provides a powerful purge. However, a quick erase of an encrypted drive also removes the keys and leaves only encrypted data behind. The problem with a quick erase is the availability of tools that can recover quickly erased macOS partitions with the recovery key (Fleishman, 2018). If an organization fails to delete the recovery key, the data is still accessible.

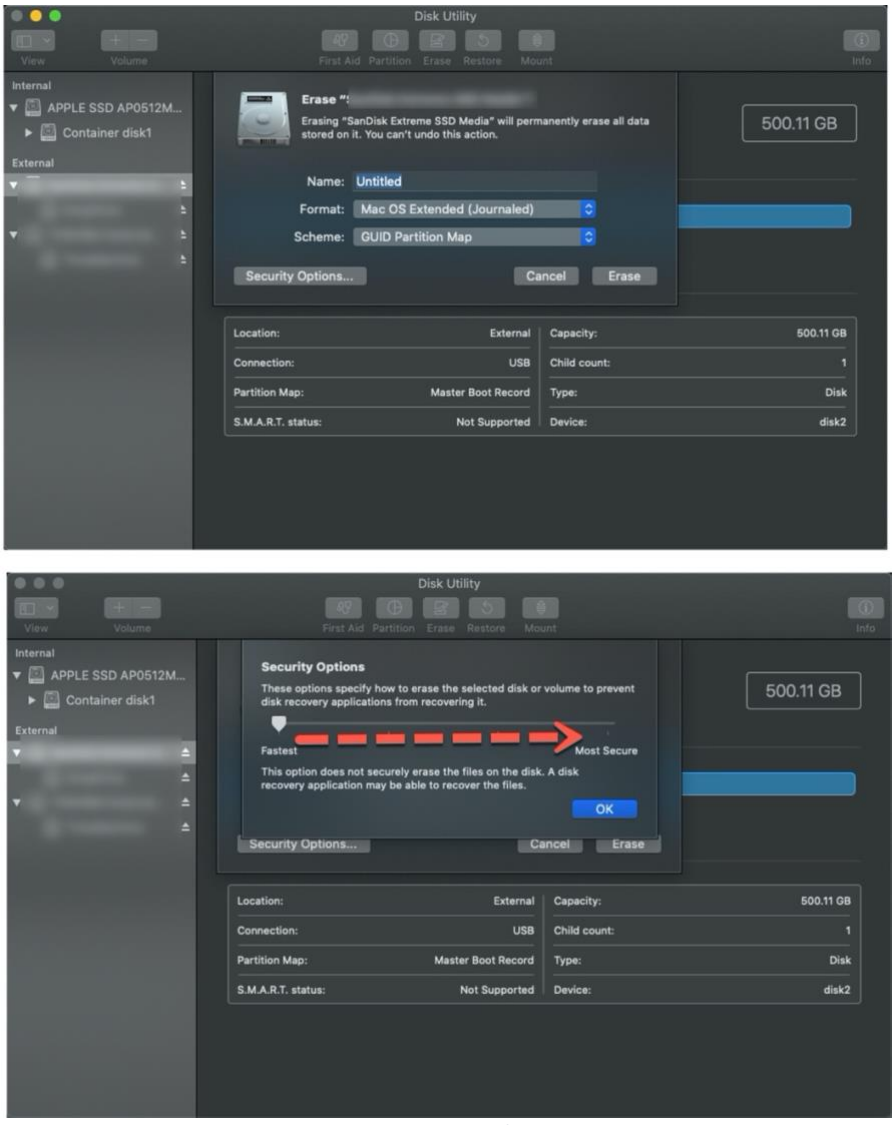

Figure 5 macOS Disk Purge

Degaussing

Degaussing is the use of a strong magnetic field to destroy the data on magnetic storage media. It can quickly erase magnetic tape and floppies. However, degaussing hard drives is not an easy process. The power applied must be sufficient for the drive purged.

Further, degaussing is not guaranteed to erase all the data. Finally, degaussing can destroy drives. If an organization plans to reuse a drive, degaussing is not a good approach.

Purchasing a degausser, maintaining it, and managing the associated purging is usually not as cost-effective as the other purging approaches described in this guide.

Destruction

When an organization retires drives containing restricted data, destruction is the best sanitization method. Risk determines the destruction approach selected.

Damage the drive

One destruction method is damaging the drive, so it cannot work when connected to a computer. Approaches include drilling a hole into the drive and using a hammer to damage the spindle. These approaches deny access to most attackers. However, attackers with access to expensive lab and forensics tools and equipment can still recover much of the data on the drive. Whether or not an organization uses this information depends on the associated risk.

Shred the drive

The most effective destruction approach is to shred drives. For example, my team collected retired drives in a secure location. Once per quarter (or more often when necessary), we transported the drives to a media destruction facility where they were shredded into small pieces. Services like Shred-it picks up an organization's drives and provides less destructive methods, such as shearing and crushing. These are usually enough for the vast majority of organizations.

Large organizations can purchase drive shredders to use on site. This requires the disposal of the shredded material. Organizations should compare the costs of purchasing and maintaining a shredder, added to the cost of material disposal, with the cost of using a service before deciding on how to approach drive shredding.

Go to Table of Contents

Solid State Drives

Wear leveling approaches on many SSDs can result in sensitive information residing in blocks where a simple overwrite would not work. Consequently, simple overwrites associated with clearing are sometimes not enough: depending on the drive and how it performs wear leveling.

Clear

Organizations can use the same approach for overwriting SSDs. Sanitization teams should only use clearing techniques when the target SSD contains confidential information. Vendors often provide tools to enable simple overwrites of entire user-accessible disk areas.

Purge

Many SSD vendors provide tools for purging their products (Constantin, 2018). Vendors design these tools to address all blocks on the drives. These tools often provide an approach that avoids overwriting. It applies a voltage spike to the drive that immediately erases all content. This avoids the overwrite process that shortens drive life. CE also works on SSDs using both self-encrypting SSDs and operating system encryption tools.

Because SSDs do not store data magnetically, degaussing does not work.

Destruction

Both crushing and shredding are proper destruction techniques for SSDs leaving the organization for retirement.

Go to Table of Contents

Paper

Large organizations have gotten the message; use a shredding service and provide employees with secure receptacles for paper copies of sensitive information. This is often not possible for SMB and home office locations. However, businesses of any size must use reasonable and appropriate methods to destroy paper documents and reports.

Shredding is the most common way to sanitize paper. Shredder manufacturers rate their devices based on the German DIN 66399 standard (DIN Standards Committee Information Tech and Selected IT Applications, 2012). See Figure 6 (Morsa, 2019).

Level	P-1	P-2	P-3	P-4	P-5	P-6	P-7
Particle Type	Strip	Strip	Cross-Cut	Cross-Cut	Micro Cut	Micro-Cut	Micro-Cut
Particle Size (Max)	Width: 0.47" Length: Paper	Width: 0.24" Length: Paper	Width: 0.08" Length: 0.5"	Width: 0.24" Length: 0.25"	Width: 0.08" Length: 0.05"	Width: 0.04" Length: 0.02"	Width: 0.04" Length: 0.01"
DIN Protection Class (1-3)	1	1	1 or 2	2 or 3	2 or 3	3	3
Rating	Very Low	Low	Medium	High	Very High	Top-Secret	Top-Secret
Certifications	None	None	None	HIPAA	HIPAA	HIPPA US Army Reg. 380-5	HIPPA NSA/CSS 02-01

Figure 6 Paper Shredder Levels

Shredders are not just for paper. Many affordable devices can also destroy optical media. If an organization internally shreds documents,n use of shredders rated at level P-3 is the minimal requirement for confidential information: level P-4 and above for restricted information.

Go to Table of Contents

Optical Media

The approaches used for optical media depend on the type of media involved. Given the cost of most optical media, destruction is likely the best option when a disc is no longer needed for data classified above public.

Clear

Overwrites are possible for rewritable optical media. Write-once and no-write optical discs do not allow clearing.

Purge

Secure Erase is not available for optical drives. However, CE is possible by not writing any unencrypted data to the disc and destroying the associated key at retirement or repurposing.

Destruction

Destruction of optical discs is straightforward: shred them. Many paper shredders rated P3 and above also shred discs.

Another approach is the use of sanders rated for disc destruction. Simply rubbing sandpaper over the top of the disc, for example, is often not enough to destroy data at all data-bearing layers.

Go to Table of Contents

Mobile Phones and Tablets

Phones and tablets today often enable the destruction of the data they contain. However, this is only possible if organizations plan and manage the devices with some level of mobile device management to ensure proper configuration.

Purge

iPhones and iPads are encrypted out-of-the-box. This means sensitive data is never written in the clear. Clearing is not practical, but purging via CE is very easy, as shown in Figure 7. By following the path in settings on an iPhone, for example, all content is made inaccessible by erasing settings, content, and encryption keys.

Encryption is not configurable by the user. Organizations using iPhones and iPads can be sure of purging effectiveness.

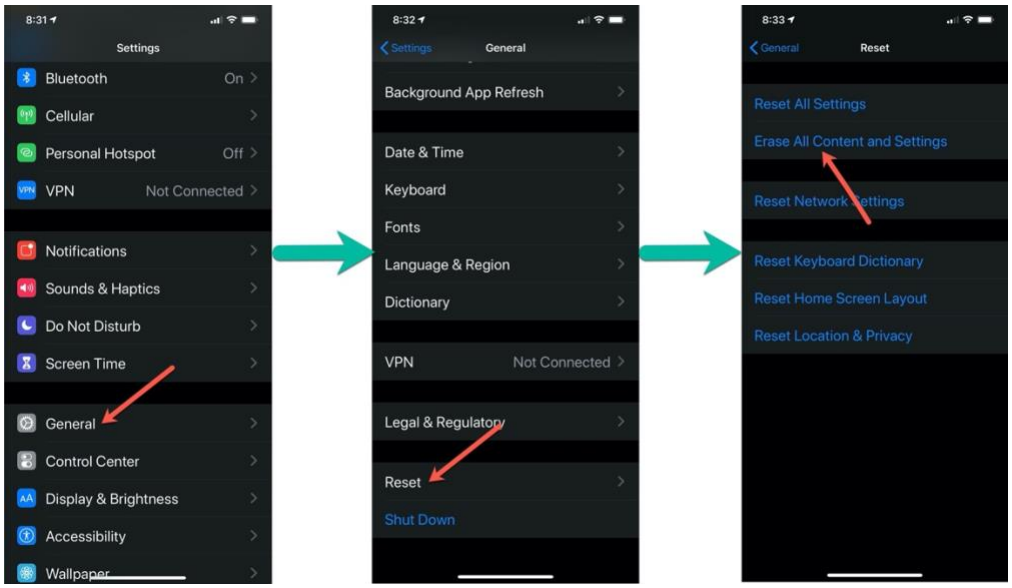

Figure 7 iPhone Purge

Google has also made it mandatory for device manufacturers that want to comply with the Android standard to include automatic encryption on all Android devices when a user configures a login PIN. However, some Android device manufacturers still do not effectively implement or support encryption(Microsoft, 2019). Users can disable encryption on devices like the Samsung Galaxy S10 from within settings (Samsung, 2019).

A factory reset of unencrypted devices will delete unencrypted information. However, there can be data remanence. To ensure CE, organizations should use mobile device management solutions, like Microsoft Intune, to force encryption on Android devices.

Many mobile devices allow the insertion of microSD or SD cards for additional storage. Managing the content of these cards is separate from managing internal storage. Encrypting storage cards is a separate process from automatic encryption when a user assigns a PIN. Further, a factory reset of the device will not affect the storage card. If a user saves sensitive information to a storage card, it is still available for extraction if the card is not removed. Refer to the microSD and SD Cards section for guidance on managing their content on reuse or retirement.

Destruction

Smashing a cell phone or tablet does not necessarily destroy the memory chips within. If an organization does not force encryption of these devices over their entire lifetimes, then they should be sent to a shredding vendor for destruction.

Go to Table of Contents

Printers and Multifunction Devices

Enterprise printers, copiers, fax machines, and multi-function devices can contain platens, magnetic disks, or SSDs. Management of magnetic and solid-state media is described earlier in this guide. Organizations should either ensure the devices include manufacturer disk purging technology or can be removed for purging/destruction. Further, some printers can be shredded by destruction vendors. Whether or not device storage can be effectively purged or destroyed is an essential consideration during acquisition.

Using robust cleaning methods on platens are usually sufficient to remove any sensitive information present in residual ink.

Go to Table of Contents

Removable USB Storage

Although some approaches to disk sanitization apply, many removable USB storage devices do not support the new sanitization methods provided by drive manufacturers. This makes these devices a separate risk consideration.

The best approach to managing these devices is to force encryption when connected. In Windows environments, this is possible with BitLocker managed with group policy. This enables cryptographic erase and provides on-the-go protection.

Users do not usually turn-in devices when no longer needed. Organizations should make it easy to dispose of USB storage by providing secure drop off points where users slide their devices

into a slot on a secured receptacle. This is similar to those provided for paper. The receptacles are then sent or picked up for content destruction. Policy, training, and management oversight are needed to manage this process.

If an organization wants to reuse USB sticks, secure erasure is possible with erase software or with devices designed for sanitization. See Figure 8.

Go to Table of Contents

microSD and SD Cards

Clearing/purging microSD and SD cards is possible with hardware erasers designed for this purpose. Figure 8 (Data Destroyers, 2019) shows some examples, including a device for erasing USB sticks. Third-party sanitization software and USB microSD/SD adapters can also accomplish this.

Organizations that prefer destruction should consider the same drop off approach described for USB storage.

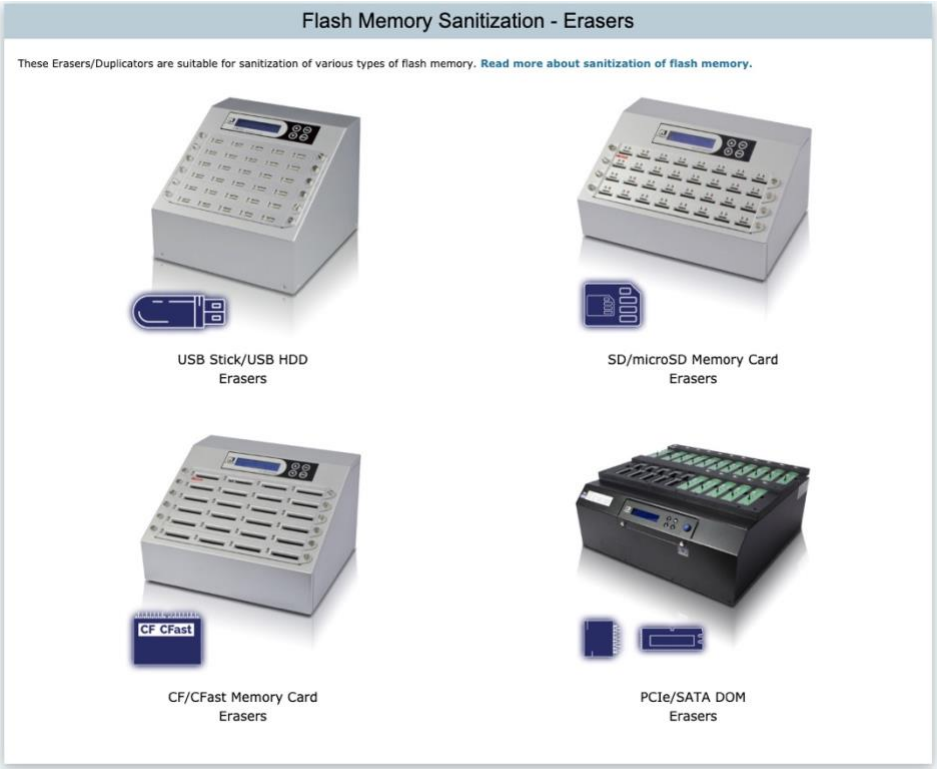

Figure 8 Flash Memory Sanitization Devices

Go to Table of Contents

EPROM and EEPROM

Hardware EPROM erasers using ultraviolet light are available for as low as $20. EEPROM is erased by applying an electric signal. These are not difficult approaches. The challenge is understanding where these devices are installed and what they contain.

For destruction, consider secure destruction bins as described for *Removable USB Storage*.

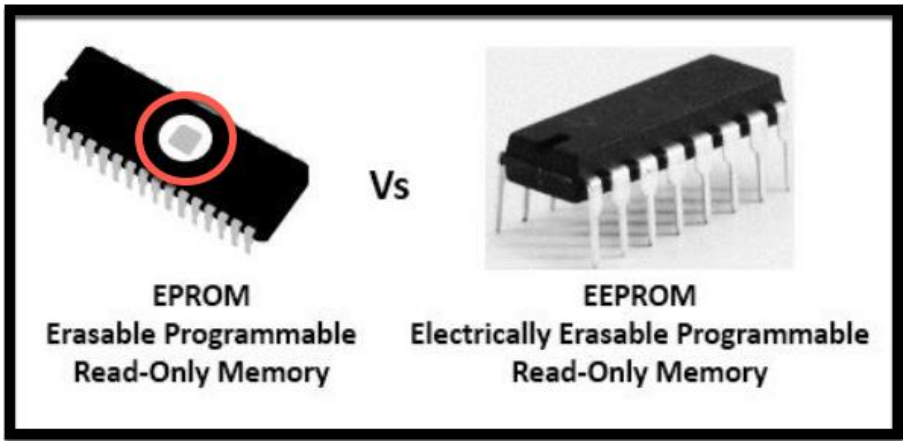

Figure 9 EPROM and EEPROM (TechDifferences, 2017)

Go to Table of Contents

Sanitization Policy and Planning

Effective sanitization requires organizations to know where and how data is stored; and the data's classifications. To accomplish this, an organization must create policy and processes integrated into system life cycles. The following steps to creating and managing a sanitization plan are based on the recommendations of the International Data Sanitization Consortium (IDSC, 2017).

Step 1. Prioritization, Scope, and Policy

The process begins by engaging with management and educating them about the risks involved with failures to sanitize media. With management buy-in, a person or team must be made responsible for sanitization outcomes.

The first step for the sanitization team is to create a checklist listing the data classification levels, on what media the data of the different levels might be located, and the sanitization approach required for reuse or disposal. When considering data locations, it is also vital to include cloud service providers and business partners. The team should use the results of this exercise to create a sanitization and equipment disposal policy draft.

The policy should include requirements for destruction audit trails. Audit trails include documents certifying successful purging or destruction of devices. Many purging products

provide a certification document upon purge. When an organization uses a third-party destruction service, it should require documentation verifying destruction and disposal.

An example policy is available from the SANS Institute. This policy is a good start, but it does not go into enough detail to cover all types of media and media-specific sanitization methods. These considerations are often unique to organizations, and sanitization teams must add or change the policy as needed to manage the risk associated with each checklist item.

Go to Table of Contents

Step 2. Orientation

The sanitization team expands the list created in Step 1 by adding any regulatory sanitization requirements. Also, risks associated with clearing, purging, and destruction sanitization of each list item are calculated: a qualitative approach is usually sufficient. The use of the formulaic model in Figure 1 is a good start to conduct item-level risk assessments.

Once risk is assigned, the team should prioritize sanitization implementations and approaches based on risk levels. The final result allows data owners to decide on the best sanitization approaches across all data/media instances. The sanitization team must ensure that data owner requirements are included in the final policy and supporting procedures. The final policy is approved by management for implementation and employee training.

Step 3. Creation of Current Profile and Gap Analysis

When conducting the risk assessments, the team should describe the current sanitization processes implemented for each list item (if any). This provides a baseline for performing a gap analysis between the current state and the required states specified by data owners in Step 2.

As the team completes a gap analysis, it should continually update an action plan prioritized by risk. Management must assign reasonable and appropriate completion dates and a person or team responsible for completing each action plan item.

Go to Table of Contents

Step 4. Apply Policies, Standards, and Procedures to the SDLC

Once an organization implements sanitization policies, IT must implement procedures to manage media across all phases of the system lifecycle. These procedures should refer to documented media standards for minimum sanitization capabilities based on the media and the classification levels of data.

1. **Initiation Phase**. Identification of data and their associated classifications help with the development of security requirements. Security requirements should specify sanitization requirements according to the organization's documented standards.

2. **Development/Acquisition Phase**. Requests for proposal for any device or any third-party service must include requirements for storage media and sanitization capabilities/procedures. When service providers (e.g., cloud service providers) will be responsible for all or some of the sanitization procedures, agreements with these providers should include documented certification of sanitization.
3. **Implementation Phase**. Change management procedures during implementation should verify the implementation of media that meet the requirements and standards set by the organization and the project team. This includes a review by the sanitization team or the security team.
4. **Operations/Maintenance Phase**. Once again, the change management process can play a big part in the sanitization efforts. A review of any changes to systems should include a review of any media changes and whether those changes comply with organization sanitization policy. The change management team should record any approved changes to media sanitization approaches or capabilities in the system documentation.
5. **Disposal Phase**. Finally, system retirement procedures should include clear documentation about how to dispose of all related media. Organizations that keep system documentation up to date should have little problem with this; the sanitization team steps through the installed media and acts according to policy and procedure.

Go to Table of Contents

Conclusion

Media sanitization is an integral part of ensuring the confidentiality of sensitive information. It is not something to which an organization pays attention only at the end of a media's usefulness. Instead, media sanitization requires consistent policy enforcement and a set of supporting procedures stretching from the planning phases of a system to its retirement.

The types of media described in this guide are only a part of what an organization might encounter. Storage is everywhere and how it is implemented and managed changes over time. The most important takeaway from this guide is understanding how to recognize and manage the risk associated with media management.

Works Cited

Best disk wiping tools for hard drives, smartphones, and SSDs. (2018, Apr). Retrieved November 2019, from Techworld: https://www.techworld.com/security/best-disk-wiping-tools-securely-cleaning-hard-drives-smartphones-ssds-3627310/

Buecker, A. (2015, Feb). *5 Things to Know About Managing Encryption Keys for Self-Encrypting Drives in Lenovo System x Servers*. Retrieved November 2019, from IBM: https://www.ibm.com/developerworks/community/blogs/5things/entry/5_things_to_know_about_managing_encryption_keys_for_self_encrypting_drives_in_lenovo_system_x_servers?lang=en

Constantin, L. (2018, Nov). *How to Securely Get Rid of Your Devices*. Retrieved November 2019, from Motherboard by Vice: https://www.vice.com/en_us/article/bjex48/how-to-securely-get-rid-of-your-devices

Data Destroyers. (2019). *Flash Memory Sanitization - Erasers*. Retrieved November 2019, from Data Destroyers: https://www.datadestroyers.eu/category/flash_memory_erase.html

DIN Standards Committee Information Tech and Selected IT Applications. (2012, Oct). *DIN 66399-1 Office machines - Destruction of data carriers - Part 1: Principles and definitions*. Retrieved November 2019, from DIN: https://www.din.de/en/getting-involved/standards-committees/nia/standards/wdc-beuth:din21:155420083

Fisher, T. (2019, Aug). *What Is Secure Erase*. Retrieved November 2019, from Lifewire: https://www.lifewire.com/what-is-secure-erase-2626004

Fleishman, G. (2018, Apr). *How to find your FileVault recovery key in macOS*. Retrieved November 2019, from Macworld: https://www.macworld.com/article/3268809/how-to-find-your-filevault-recovery-key-in-macos.html

IDSC. (2017). *7 Steps to Create a Data Sanitization Policy*. Retrieved November 2019, from IDSC: https://3ts8wr3gbhb94e74ina1ic43-wpengine.netdna-ssl.com/wp-content/uploads/2017/08/7-steps-to-create-a-data-sanitization-policy-ebook.pdf

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014, Dec). *Guidelines for Media Sanitization, SP 800-88 rev1.* Retrieved October 2019, from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

LSoft Technologies Inc. (2019). *NTFS Journaling*. Retrieved November 2019, from NTFS.com: https://www.ntfs.com/transaction.htm

Microsoft. (2019, Apr). *Encrypting your Android device*. Retrieved November 2019, from Microsoft Intune User Help: https://docs.microsoft.com/en-us/intune-user-help/encrypt-your-device-android

Morsa, M. (2019, May). *Shredder Particle Sizes: A Comprehensive Guide*. Retrieved November 2019, from Binding 101: https://www.binding101.com/resource-center/shredder-particle-sizes

Olzak, T. (2012, Jan). *Risk Management - Chapter 2*. Retrieved November 2019, from InfoSec: https://resources.infosecinstitute.com/risk-management-chapter-2/

Samsung. (2019, Aug). *How do I decrypt my phone with encrypted security notice?* Retrieved November 2019, from Samsung: https://www.samsung.com/nz/support/mobile-devices/how-do-i-decrypt-my-phone-with-encrypted-security-notice/#:~:targetText=1%20Open%20Settings%20on%20your,Strong%20protection%20to%20disable%20encryption.

TechDifferences. (2017, Feb). *Difference Between EPROM and EEPROM*. Retrieved November 2019, from TechDifferences: https://techdifferences.com/difference-between-eprom-and-eeprom.html#:~:targetText=EEPROM%20is%20an%20Electrically%20Erasable,erased%20by%20the%20electrical%20signals.