SECURE ENTERPRISE ASSET MANAGEMENT

CHOOSING THE RIGHT DATA DESTRUCTION METHOD

When electronic equipment is no longer needed, destruction of the data contained is critical, and often required. With the highly advanced recovery techniques of today, data can be easily recovered from devices that have been improperly wiped or destroyed.

Many companies make the choice to utilize in-house resources for data erasure and destruction, but if the process is not strictly enforced and audited, hard drives and equipment may be lost, stolen or misplaced. Having a well managed data security policy in place with a certified data destruction partner helps create accountability and accuracy. Organizations must make risk-based decisions on which data destruction method to choose depending on the type of data and potential harm if exposed.

DELETE / REFORMAT: Deleting or reformatting information is not effective. This method removes only pointers to information on the device, not the actual digital data which can be easily retrieved.

WIPE: If performed correctly, wiping effectively erases data while maintaining device functionality for reuse or resale. With this method, each drive sector is rewritten several times over with random data to ensure it is cleared. Wiping allows for auditable reports in compliance with federal and industry standards. However, professional software and skilled technicians are required to ensure all information is effectively erased. This method is not an option for damaged drives.

DEGAUSE: Degaussing uses a very strong magnet to randomize the alignment in magnetic devices such as tapes and hard drives, leaving data unrecoverable. This method can be very expensive and renders the device itself useless, meaning reuse or resale is no longer an option. With solid state drives becoming more popular, this method is becoming obsolete as SSDs do not store data magnetically.

DRILL / BEND / CRUSH / HAMMER: Drilling, bending, crushing and/or hammering are not effective data destruction methods. The platter or storage chips in the device may not be 100% damaged, as a result, the data can be recovered using forensics software.

SHRED: Shredding physically grinds devices into hundreds of smaller pieces, rendering it completely inoperable and effectively preventing any recovery of data. The disadvantage of shredding is that it prevents any opportunity for reuse or resale. Shredding requires professional equipment capable of destroying the selected media type. If destruction is not performed correctly, data may be recovered from the individual fragments.

An effective data destruction strategy ensures security, maximizes return and minimizes business risk. The only sure way to accomplish this is through a certified, auditable process that abides by proper policies and procedures.

At SEAM, we understand the liabilities that come along with managing data. We work with businesses of all sizes to help them comply with data security requirements and regulations in Finance, Healthcare, Retail, and Education. Our certified services provide verifiable proof of data erasure and/or destruction to protect you, your company, and your customers.

Contact us to learn how we can manage the risk so you don't have to.

SEAMSERVICES.COM

605-274-SEAM (7326) | SIOUX FALLS, SD