Safely and securely claim the residual value of your organization's retired IT assets

Sanitize or destroy; either way 100% secure, compliant and absolute. On site service!

ZERØtrace

leave nothing behind

CODs issued by serial; verifiable proof that your organization is fully compliant and audit ready!

CERTIFIED DATA SANITIZATION AND DESTRUCTION SERVICES

ZERØtrace, LLC.

4062 Watts St.
Emeryville, CA 94608

Toll Free: (800) 992-4135

solutions@zer0trace.com

www.zer0trace.com

TYPES OF SANITIZATION - **Clear, Purge, and Destroy**

Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple noninvasive data recovery techniques.

When:

- Hardware remains relevant and in good condition; redeploy extending return on investment

How:

- Utilize standard Read/Write commands to rewrite with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

Purge applies physical or logical techniques that render target data recovery infeasible using state-of-the art laboratory techniques.

When:

- Hardware will be returned to lessor at end of lease
- Hardware has residual value and can be sold to offset replacement cost

How:

- Overwrite (aka wipe; erase) the storage media with new data utilizing specially developed and certified destruction software. NIST recommends a single-pass 0x00 overwrite, however, specific overwrite patterns and multiple passes are available upon request including many popular 3-pass patterns and the seven-pass pattern: 0xF6, 0x00, 0xFF, random, 0x00, 0xFF, random; sometimes erroneously attributed to the US standard DOD 5220.22-M.

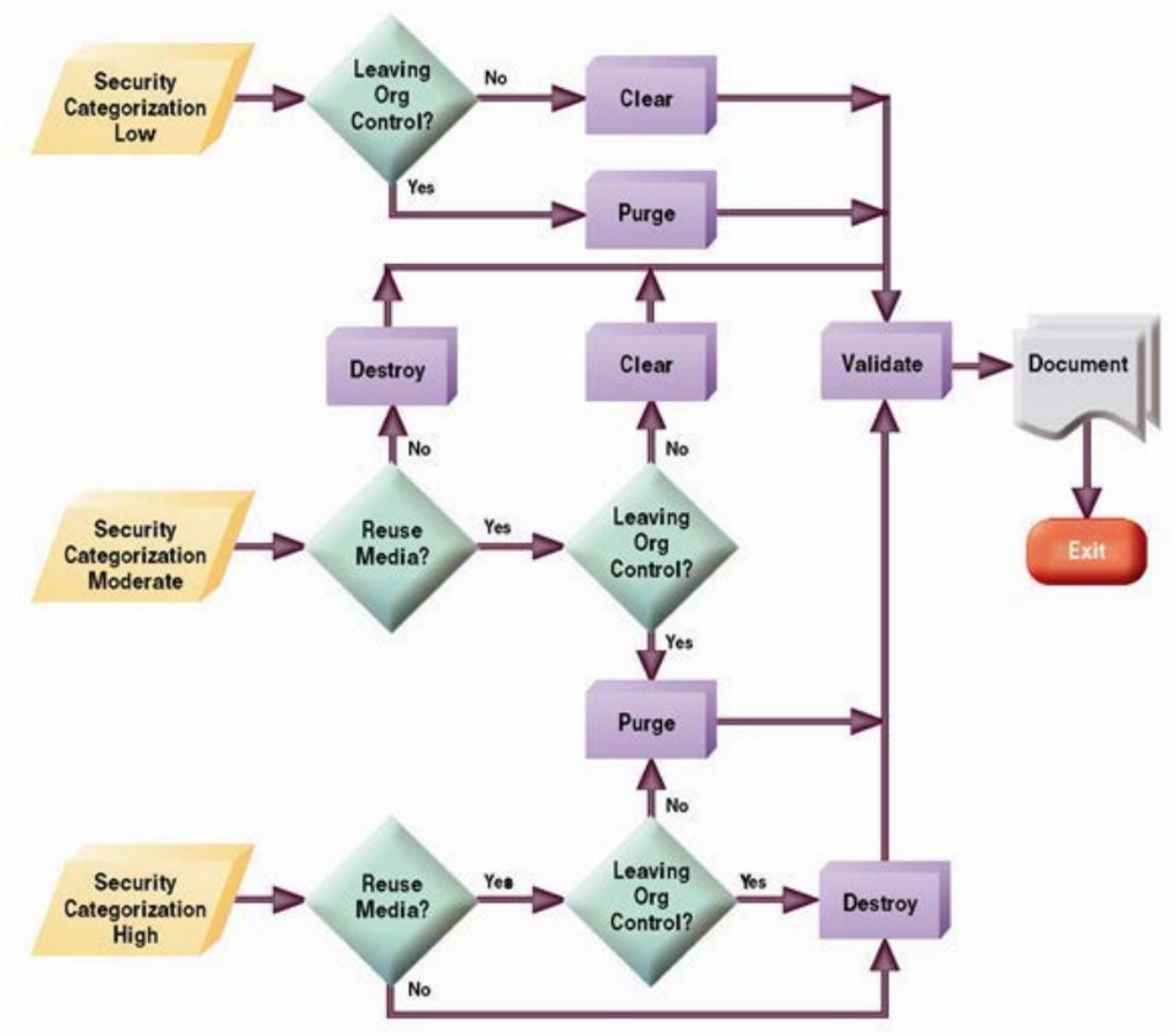
Destroy renders target data recovery (using state-of-the-art laboratory techniques) infeasible and results in the subsequent inability to use the media for storage of data.

When:

- Hardware is obsolete, has no further use or value or is damaged; recycle raw materials
- Contains extremely sensitive or classified information
- Mandated by corporate/company/agency rule/policy

How:

- Degaussing with certified and approved high volume capacitive discharge degaussers to completely and permanently erase all data, including failed or damaged hard drives regardless of OS or interface.
- Shred media into remnant particles sized to ensure any forensic attempt to recover data is precluded. 1.5” particles for HDDs; .375” particles for flash memory based storage media (SSDs, mobiles devices, USB sticks, DIMMs, etc.)



NUMBER OF OVERWRITE PASSESS FOR MAGNETIC MEDIA

According to the 2014 NIST Special Publication 800-88 Rev. 1, Section 2.4 (p. 7): " For storage devices containing magnetic media, a single overwrite pass with a fixed pattern such as binary zeros typically hinders recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data."

According to the 2006 Center for Magnetic Recording Research Tutorial on Disk Drive Data Sanitization Document (p. 8): "Secure erase does a single on-track erasure of the data on the disk drive. The U.S. National Security Agency published an Information Assurance Approval of single-pass overwrite, after technical testing at CMRR showed that multiple on-track overwrite passes gave no additional erasure."

Further analysis by Wright et al. in *Overwriting Hard Drive Data: The Great Wiping Controversy* concludes that "…there is minimal (less than 0.01% chance) of recovering data on a NEW and unused drive that has a single raw wipe pass (not even low-level format). In the cases where a drive has been used (even being formatted for use) it is not possible to recover the information"

While ZER0trace recommends a single-pass approach in light of lab test data showing this approach to be fully secure; we fully support any wipe pattern standard our customers prefer. The cost benefit analysis should be considered by each organization.

OVERWRITE TIME CALCULATIONS

Write speed testing for modern enterprise storage drives published by Tom's Hardware shows a range of write throughput between 70 and 220 MBp/s. Using a 4 TB SATA drive as an example, time to complete overwriting taking into consideration low, average and high throughput rates when conducting single, three and seven pass patterns:

Drive Capacity (MB)	Avg. Write Throughput (MB/s)	Estimated Seconds per pass	Estimated Minutes per pass	Estimated Hours per pass	Number of Passes	Total Hours
4,096,000	210	19505	325	5	1	5
4,096,000	140	29257	488	8	1	8
4,096,000	70	58514	975	16	1	16

Drive Capacity (MB)	Avg. Write Throughput (MB/s)	Estimated Seconds per pass	Estimated Minutes per pass	Estimated Hours per pass	Number of Passes	Total Hours
4,096,000	210	19505	325	5	3	16
4,096,000	140	29257	488	8	3	24
4,096,000	70	58514	975	16	3	49

Drive Capacity (MB)	Avg. Write Throughput (MB/s)	Estimated Seconds per pass	Estimated Minutes per pass	Estimated Hours per pass	Number of Passes	Total Hours
4,096,000	210	19505	325	5	7	38
4,096,000	140	29257	488	8	7	57
4,096,000	70	58514	975	16	7	114

The calculation table clearly shows that the level of effort in time and resources to complete multiple passes is significant. Careful consideration between perceived additional security and actual resource investment is highly recommended.

FLASH MEMORY BASED STORAGE MEDIA CONSIDERATIONS

Media technologies, such as flash memory-based storage devices including Solid State Drives (SSDs) and self-encrypting drives, have become prevalent. Degaussing and overwriting techniques - common methods for sanitizing magnetic media - are not applicable for flash memory devices. Storage devices with integrated encryption and access control capabilities, also known as Self-Encrypting Drives (SEDs) feature always-on encryption that substantially reduces the likelihood that unencrypted data is inadvertently retained on the device. At ZER0trace, we utilize certified overwrite software specifically designed for SSDs. These tools leverage essential internal erasure commands to secure SSDs, including Cryptographic Erase (CE), include multiple overwrites, freeze lock removal and full verification.

SUMMARY SANITIZATION OPERATIONAL SERVICE DESCRIPTION:

1	ZER0trace arrives at customer location with mobile sanitization lab; appliances and overwrite software utilities best suited to physical and communication architecture.
2	Inventory (barcode scan) and document all items presented for sanitization.
3	Customer determines desired overwrite scrutiny; primary service includes NIST SP 800-88 Rev. 1 single-pass overwrite (all 0s), however, several other options are available, including the popular U.S. DoD 5220.22-M(E), HMG IA Std. 5(E), and CSEC ITSG-06 three-pass standards.
4	Loose drives are loaded into compatible chassis infrastructure designed for executing bulk sanitization jobs; storage array disk bays are directly connected to our sanitization appliance where overwrite can be launched against all drives on the connected bus.
5	When sanitization overwrite is complete, verification is conducted to ensure all sectors and hidden areas have been overwritten, provides a defects log list and list bad sectors that could not be overwritten.
6	After passing verification, a certificate of destruction is created that includes time/date, make/model, serial, description (i.e., magnetic, flash memory, hybrid, etc.), media source (system of origin), sanitization utility used (including version), verification method (i.e., full, quick sampling, etc.), name/title/signature of ZER0trace technician.
7	Networking equipment, mobile devices, etc. are scrubbed of configuration data and factory defaulted; any physical asset tags or owner identification labeling is removed.

SUMMARY DESTRUCTION OPERATIONAL SERVICE DESCRIPTION:

1	ZER0trace arrives at customer location with mobile destruction truck equipped with degausser and high capacity shredders specifically set up to demagnetize and then shred HDDs into .750” particles and SSDs, mobiles devices and flash-memory based media in to .375” particle sizes.
2	Inventory (barcode scan) and document all items presented for destruction.
3	Individual items are degaussed inside your facility then transported out to the destruction truck OR to Emeryville, CA destruction plant via secure chain of custody and GPS tracking.
4	Individual items are scanned again as they are deposited into the shredder. Closed Circuit Video cameras record the scan and drop, as well as the item being shredded. Additional cameras record all areas within the truck simultaneously. Video footage of each item destroyed is retained and provided with CODs.
5	Electronic CODs are posted to customer portal along with video footage. Customer can access via web browser as well as iOS/Android mobile device. Paper certificates, as well as notarization, are available as well.

SPECIFIC DATA SANITIZATION AND DESTRUCTION PROCESS AND METHODOLOGY:

MAGNETIC MEDIA:

Floppies, magnetic disks (flex or fixed), reel/cassette magnetic tape	
Sanitize	N/A, recycle raw materials
Destroy	Degauss and shred
Hard Disk Drives – IDE, PATA, SATA, eSATA, SCSI, SAS, FIbre Channel, UAS and SCSI Express	
Sanitize	Writeable sectors are sanitized by overwrite process via certified utility (Blancco, Xerase, WipeDrive). Overwrite is verified upon completion and once passed, we then issue a unique certificate of destruction that includes make, model, serial and system of origin.
Destroy	Degause and/or shred each disk into ¾"particles thoroughly and completely destroying the platters. Unique certificate of destruction issued by device ID (make, model, serial, system of origin). Shredding is video recorded.

FLASH MEMORY BASED MEDIA:

Solid State Disk Drives, External attached (USB, Firewire), NVM Express, Thumb Drives, Pen Drives, SD, SDHC, MMC, CF, MicroSD, MemoryStick, Embedded Flash Memory on motherboards and devices, etc.	
Sanitize	Writeable sectors are sanitized by overwrite process via ADISA-approved utility (Blancco or BCwipe). Upon overwrite success verification, unique certificate of destruction that includes make, model, serial and system of origin is issued.
Destroy	Destroy by shredding to 3/8" particle standard

RAM & ROM-BASED STORAGE DEVICES:

DRAM, Electronically Alterable PROM (EAPROM), Electronically Erasable PROM (EEPROM)	
Sanitize	Purge existing configuration data and execute full restoral to factory defaults per manufacturer instructions. Remove any/all physical identification or asset tracking.
Destroy	Destroy by shredding to 3/8" particle standard

NETWORKING DEVICES:

Routers, Switches, Load Balancers, Firewalls, Optimization & Security Appliances	
Sanitize	Power down device, remove power source, and battery (if battery backed) or remove DRAM from device. Perform chip purge per manufacturer data sheets (EAPROM). Overwrite with manufacturer provided default configuration/reset (EEPROM).
Destroy	PCB / motherboard removed and shredded to 3/8" particle standard; remaining hull material shredded for recycling. All magnetic or flash memory storage elements removed and sanitized or destroyed IAW appropriate classification.

MOBILE DEVICES:

Apple iOS, Android OS, Blackberry OS, Windows Phone, etc., mobility devices	
Sanitize	Execute full sanitize option within settings; reset to factory defaults IF device accessible; by EIN or S/N through manufacturer support channels for locked no credential units
Destroy	Shredded to 3/8" particle standard; any removable storage (memory cards, SIMs) to be sanitized and/or destroyed IAW appropriate classification.

OFFICE PERIPHERAL AND INTERNET OF THINGS (IOT) DEVICES:

Copiers, printers, multifunction machines, firestick, AppleTV, etc.	
Sanitize	Execute full sanitize option within settings; reset to factory defaults. HDD or SSD onboard storage processed IAW with appropriate classification.
Destroy	Shredded to ¾" particle standard or crushed via hydraulic press as form factor dicates; HDD or SSD onboard storage processed IAW with appropriate classification.

OPTICAL MEDIA:

CD, DVD, BluRay Disc	
Sanitize	N/A, recycle raw materials
Destroy	Cross cut shredding