

## DIGITAL SHREDDER MANUAL OVERVIEW SHEET



### SYSTEM CONFIG

- **After logging in, the user is presented with the System Config screen**
- This is the main screen from which all menus can be accessed

### USERS

- **The Digital Shredder has two user levels :administrators and operators**
- User permissions vary depending on user level
- The user screen allows an administrator to add, edit or remove users
- **Administrators also have full unit control** including the ability to **export** or **purge log data** and **set process** defaults

### SET DATE/TIME

- **This screen allows for the date and time to be set**
- To set the date and time, press the “today” button on the bottom of the screen and adjust the fields as necessary/Press save

### PRINTER

- **The printer button located at the bottom left is used to configure the printer**
- This screen allows the user to perform a test print

For More Info



### HISTORY

Click Here --->

- **The history screen is used to access the audit log**
- All machine activity is stored in this log
- The log contains general machine activity such as logins and logouts as well as information on every hard drive that has been decommissioned by the machine
- The log entry includes the hard drive serial number, operator username, the erasure process used and the date and time of the beginning and end of the operations
- All log data can be exported by an Administrator in CSV format to a USB drive by using the USB port on the back of the machine

### UPDATE

- **When software updates for the Digital Shredder are released by EDT, they can be installed by using the update screen**
- Software updates are available for download from EDT’s corporate website
- Simply download the update file, load it to a USB drive and place it in the USB port on the back of the machine
- When the USB drive is recognized , click the update button in the bottom right corner of the screen to update the software

### RESTORE

- **The restore screen allows the user to restore the machine to an earlier software version should an update not install correctly**

<http://www.monomachines.com/Digital-Data-Destruction/HSM-DS-200-Digital-Shredder.htm>

## DEFAULT OPS

- **The default ops screen allows a user to set the default operations that will be executed on a drive when it is inserted into a drive bay**
- Insert a drive and simply select the “Run” button without having to select the individual operations for each drive that is inserted into the machine. This saves considerable time when processing multiple drives
- However, the user also has the ability to vary from the default operations on any drive
- **The operations available include: Use Secure Erase if possible , use default overwrite method , create default partition, disk image and print certificate**
- The “Use Secure Erase if possible” setting will Secure Erase the drive when possible
- If Secure Erase is not available , The Digital Shredder will proceed to the next selected operation
- The “Use default overwrite method” allows for the user to select a standard overwrite routine
- The ”Create default partition” creates a single partition equal to the maximum storage capacity of the drive
- **If “ Create default partition” is selected , the user can choose the “Format disk” option and select the file format for the partition**
- File formats available include FAT16, FAT32,NTFS,EXT2 and EXT3
- The “Disk Image” setting allows for the drive to be imaged using a source drive located in another bay
- The source drive must be inserted in the far right drive bay
- **The final menu item is the “Print Certificate “ setting**
- When this option is turned on, a printed certificate is produced when the operations are completed
- If this option is off. the Digital Shredder will still store all decommission information which can be printed at a later date

## OPERATIONS

- **The operations screen visually represents the three drive bays**
- When a drive is inserted , the hard drive`s serial number will appear above the corresponding bay
- When the bay is selected, the user is presented with the default ops screen
- Here, the user can review the operations about to be executed on the drive and then run them by selecting the “Run” button at the bottom of the screen
- **After selecting “Run” , the user can check the status of the drive in two ways**
- First , an estimate of the completion percentage is displayed on the screen above the relevant drive bay
- Second, a LED indicator in the drive bay indicates the drive`s current status
- When the LED is off, the bay is available for use
- A Green LED indicates that a drive is loaded and ready but no operation is taking place
- A Blinking Green LED indicates that the operations executed on the drive are complete and the drive can be ejected
- A Red LED indicates tha an erasure operation is currently being executed. During this time the drive is mechanically locked and password protected
- An Orange LED indicates that the drive is being reformatted or re-imaged

# SIMPLE OPERATION



## Connect the hard drive to the plug adapter.

- ATA/IDE and SATA hard drives are supported (2.5" and 3.5").
- Robust interface with long service life.
- No irritating connection cables.



## Insert the plug adapter with the hard drive into a drive.

- You can wipe hard drives simultaneously in all three drives.
- The drives are locked and password-protected.



## Activate the erase process.

- The Secure Erase technology destroys the data completely, making it impossible to restore it even with forensic methods.
- There are no charges for the software licence. You can download updates from the internet and install them using a USB connection.



## Print the deletion log.

- Thorough documentation of the process: The serial number of the hard drive, name of the operator, and type and duration of the erase process are documented.
- The label printer is included in the scope of delivery.

<http://www.monomachines.com/Digital-Data-Destruction/HSM-DS-200-Digital-Shredder.htm>

For More Info

Click Here --->



**WWW.DIGITAL-SHREDDER.DE**



# Erasing hard drives - quick, simple and absolutely secure -

For More Info



Click Here --->

# HSM<sup>®</sup>

HSM GmbH + Co. KG  
Bahnhofstr. 115  
88682 Salem

Tel. +49 (0) 75 53 / 822-0  
Fax +49 (0) 75 53 / 822-160

[www.digital-shredder.de](http://www.digital-shredder.de)



**DIGITAL  
SHREDDER**  
powered by **EDT**

<http://www.monomachines.com/Digital-Data-Destruction/HSM-DS-200-Digital-Shredder.htm>

# Topic

For More Info

Click Here ---->



- Sensitive information is not always stored on paper.
- Nearly everywhere nowadays, sensitive information is stored on hard drives; this includes personal data, research and development data, corporate strategies and much more besides.
- The dangers of careless handling of this data are well known from the field of document shredding: identity theft, loss of corporate know-how and business data.



# Market

For More Info

Click Here --->



## ❑ Facts and figures

- 96% of all companies in Europe use computers – at companies with more than 250 staff this figure rises to 100%  
(Source: eurostat)
- Only 33% of 400 used hard drives bought on eBay were securely erased – of the other data media, it was possible to restore some highly sensitive information, such as web access data for the US Air Force (Source: Heise online, Test of O&O)

# Market

For More Info

Click Here ---->



## ❑ When is it necessary to erase a hard drive?

- When taking old PCs, laptops, printers, photocopiers and fax machines out of service or returning them to leasing companies
- When reassigning PCs and laptops within the company (e.g. from Design to Sales)
- Virus attacks



# Market

For More Info

Click Here ---->



❑ What methods are there on the market for removing data from hard drives?

➤ Deleting

Only the path is deleted, not the data itself

➤ Overwriting

Software overwrites the data x times

- Not all sectors on the disk are detected
- Time-consuming
- Quite complicated for non-IT-experts → This can lead to errors
- No proof of whether deletion was successful



# Market

For More Info

Click Here ---->



❑ What methods are there on the market for removing data from hard drives?

➤ Demagnetising

The (magnetically stored) data is erased using a strong magnetic field

- No guarantee that the data has been deleted
- The disk cannot be used again



➤ Physical destruction

- Often done by third parties → No control over one's own data, storage and shipping are not secure



# Product

For More Info

Click Here --->



## The Digital Shredder is a standalone solution for reliably wiping hard drives



# Product

For More Info

Click Here --->



- The Digital Shredder utilises an command of the hard drive manufacturer called “Secure Erase” to delete the data

## Secure Erase

- Initiated by the National Security Agency (NSA)
- Developed and certified by the Center for Magnetic Recording Research (CMRR), San Diego and the University of California
- Integrated on nearly all hard drives since 2002

# Product

For More Info

Click Here --->



## Digital Shredder

- Direct access to “Secure Erase” (not possible on PCs during normal operation)
- No comparable competitor currently on the market
- Used among others by the
  - National Security Agency (NSA)
  - Royal Canadian Mounted Police (RCMP) and the Canadian government
- Tested and verified by various forensic institutes (e.g. State Crime Labs) and companies

# Product

For More Info

Click Here --->



- ❑ When “Secure Erase” is activated, the hard drive is overwritten. However, compared to normal overwriting, this process is
  - *More secure:* even defective sectors are erased, a deletion log is created and a successful process is guaranteed
  - *Faster:* 3 hard drives simultaneously, 8 times faster than conventional overwriting software
  - *More user-friendly:* no special skills needed, easy to use

# Product

For More Info

Click Here ---->



## **Secure Erase meets the demands of the following US Government and Military Policy Guidelines and Directives:**

- Department of Defense (DOD NISPOM) 5220.22-M
- Deputy Secretary of Defense Memo dated May 29, 2001;  
Subject: Disposition of Unclassified DoD Computer Hard Drives,  
signed by Paul Wolfowitz
- National Computer Security Center (NSCS-TG-018); Rainbow  
Series "Light Blue Book" - A Guide to Understanding Object  
Reuse in Trusted Systems
- National Computer Security Center (NCSC-TG-025); Rainbow  
Series "Forest Green Book" - A Guide to Understanding Data  
Remanence in Automated Information Systems

# Product

For More Info

Click Here ---->



- National Institute of Standards and Technology (NIST) SP 800-88 - Guidelines for Media Sanitization
- National Institute of Standards and Technology (NIST) SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- United States Air Force System Security Instructions 5020
- United States Army AR380-19
- United States Navy Staff Office Publication (NAVSO P-5239-26)
- United States Navy OPNAVINST 5239.1A

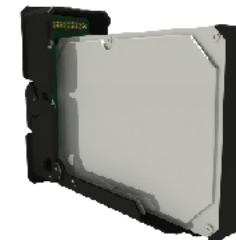
# Product

For More Info

Click Here --->



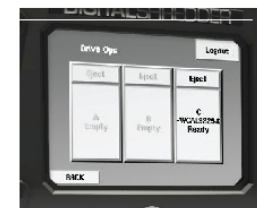
1. Plug the hard drive into the matching adapter  
All formats supported, sturdy connectors



2. Push the adapter into the drive  
3 drives can be used at once, closed drive is password-protected



3. Activate "Secure Erase"  
The hard drive is erased and simultaneously formatted for re-use



4. Print the certification label  
To subsequently show who erased what and when, and whether the procedure was successful



# Erasing hard drives - quick, simple and absolutely secure -

For More Info



Click Here ---->



# HSM<sup>®</sup>

HSM GmbH + Co. KG  
Bahnhofstr. 115  
88682 Salem

Tel. +49 (0) 75 53 / 822-0  
Fax +49 (0) 75 53 / 822-160

[www.digital-shredder.de](http://www.digital-shredder.de)

## Referenzen // References

### US GOVERNMENT / MILITARY

The Digital Shredder Secure Erase device meet and / or supports the following Department of Defence or Civilian Government guidelines concerning Information Security Practices:

- **Deputy Secretary of Defense Memo** dated May 29, 2001; Subject: Disposition of Unclassified DoD Computer Hard Drives, signed by Paul Wolfowitz
- **National Computer Security Center (NCSC-TG-018)**; Rainbow Series "Light Blue Book" - A Guide to Understanding Object Reuse in Trusted Systems
- **National Computer Security Center (NCSC-TG-025)**; Rainbow Series "Forest Green Book" - A Guide to Understanding Data Remanence in Automated Information Systems
- **National Institute of Standards and Technology (NIST) SP 800-88** - Guidelines for Media Sanitization \*
- **National Institute of Standards and Technology (NIST) SP 800-14** - Generally Accepted Principles and Practices for Securing Information Technology Systems
- **United States Air Force System Security Instructions 5020**
- **United States Army AR380-19**
- **United States Navy Staff Office Publication (NAVSO P-5239-26)**
- **United States Navy OPNAVINST 5239.1A**





## Dead on Demand Digital Shredder

This document provides information on the Digital Shredder provided by EDT. The device was tested for its usefulness within ICE. The Shredder provides secure erase high-speed data deletion for a wide variety of hard disks. The Shredder is capable of erasing up to three drives simultaneously and is capable of erasing multiple drive formats. In addition the Shredder can transfer an approved image from one of the drives to the other two bays. The Shredder is a portable and secure device for hard disk erasure.

### Ease of setting up

The Digital Shredder comes fully pre-configured and ready for use out of the box. The Digital Shredder requires a standard power outlet in order to power the device. The printer is powered by a rechargeable battery or AC adapter, and connects to the Digital Shredder via a client only USB port. Initial access to the device is controlled via a default username and password configuration which is changeable. The Digital Shredder is NOT able to be connected to a network. Updates to the operating system are accomplished via a standard USB thumb drive, ScanDisk currently are the only drives that are recommended for use.

### Initial Settings

Once you have logged into the Digital Shredder you are presented with the Administrative screen, this screen consists of the following selectable areas:

- Users – Creation and removal of users to the Digital Shredder
- Set Date/Time – Allows you to set the date and time on the Shredder
- Update – This is where you update the firmware on the Shredder
- History – This is where you view the audit trail from the device, to see any action performed on the Shredder and the user who made the action.
- Default Ops – Allows you to set the default operations for the Shredder
- Restore – This allows you to restore a previous version of the firmware.
- Operations – This is where you are able to erase your drives.

By design only admin's are able to perform the above actions, default users are only able to access the drive erase functions.

### Establishing a connection

Initial connection is made with the default admin/password. There is no method for connecting these Shredders to a network nor is there a way to connect the Shredder to another device via the USB port.

### Recommendation:

I would recommend that ICE consider utilizing the EDT Digital Shredder. The EDT product provides reliable and speedy removal of sensitive ICE data from standard hard disks. With the upcoming release of their SCSI and USB blocks this solution will provide ICE with complete coverage for all media.\*

For More Info

[Click Here --->](#)

\*note, CDR's and DVD's were not covered as part of this evaluation.



## Digital Shredder vs. Shredding / Degaussing

If physical destruction practices effectively address the need for absolute data sanitization, then why create Secure Erase?

In order to position Secure Erase in the world of Physical Destruction, an understanding of the operation and function of physical destruction technologies should be clear. If we consider two means to destroy legacy hard disk based storage devices, Shredding and Degaussing, both technologies rely on 'no contact' practices that invoke physical damage to the storage device in an attempt to render the data unrecoverable. In the case of Shredding, the entire device including the media is mechanically chipped into small fragments. Whereas, degaussing involves the application of magnetic energy to the storage device, with the expectation that the device once processed will be rendered inoperative, and that the media will not contain any recoverable data. Ultimately, neither solution accommodates the ability to re-use the decommissioned asset, and contribute to the mass of e-waste being generated.

**SHREDDING / DISINTEGRATION** The practice of shredding has a specific environmental impact requiring the resulting waste to be sorted into appropriate waste types so that circuit board, chassis alloy, platter alloy, magnetic, and electronics can be processed in an environmentally acceptable manner. This process adds significant cost to the service provider and ultimately to the consumer. From the aspect of liability, the client should be concerned with the resulting particulate size of the processed product, and the value of the data that had been stored on the destroyed device. These factors are very pertinent to evaluate whether data can be reconstructed from the shredded particles, and if anyone will afford such effort to this endeavor<sup>1</sup>.

As the device is reduced to particles, the data is considered un-reconstruct able due to the state of the device, despite no alteration to the data contained on the now shredded platters.

**DEGAUSSING** The effectiveness of degaussing is relative to the strength of the magnetic field used, and the chemistry of the platter media. For degaussing to provide assured effectiveness, field strength, direction, signal attenuation due to casing and mechanical obstructions must be addressed. Furthermore, effective data destruction cannot be claimed where cursory damage is achieved, without assured eradication of data from the media. As such, degaussing when not performed effectively can actually afford the user a false sense of security, as the damage done by degaussing only disabled the drives mechanics, electronics, or the Servo track. Each of which laboratory efforts will effectively result in restored data.

As a 'no-touch' technology, degaussing does not afford the user the ability to validate whether the data contained on the tracks of a processed device is in fact unrecoverable. Add to this the fact that the power of degaussing devices needs to be sufficient to achieve effective coercion of the magnetic polarization of the subject media, and that as platter media chemistry technology continually delivers improved higher density media; the power that a degausser must present to the subject device needs to increase in step. Understandably, it is now necessary to present 11,000 oersted to effectively degauss most modern high capacity devices, with an understanding that ultra high capacity or multi-platter storage devices requiring up to 15,000 oersted. In either case, those that employ the practice of degaussing either in house, or off site, will need to regularly upgrade their degaussing technology to deliver the surety of the process to the owner of the data.

As the power of these devices increases, the suitability of the use of these appliances in the office or enterprise will require facilities to process these devices that will assure no resultant health risk, or

---

<sup>1</sup>According to the University of California's Center for Magnetic Recording Research, a shredded particle is deemed irrecoverable when the particle size is smaller than the area necessary to accommodate a complete 512kb Sector. This area diminishes as the density of platter media increases. According to their last reported results, this area was reported to be smaller than 1/125th of an inch.

## Digital Shredder vs. Shredding / Degaussing

DIGITALSHREDDER

powered by **EDT**

Electro Magnetic Interference with other equipment. It is for this reason many enterprise clients choose to employ off-premises destruction.

In data destruction it is critical to state with certainty that the data that was on the device is now purged with certainty. The potential for data reconstruction is not an option; the process must be effective and provide provable results. Relying on mechanical disability as the criteria for determining a device being non-recoverable does not assure this certainty, and will pose a liability for the party performing the service. For service providers and manufacturers to accurately assure effective data destruction beyond forensic reconstruction, they must test their process to the specific hardware that they will be processing for their client, and have the sample devices analyzed thoroughly at a laboratory for effective and complete coercion of all sectors and regions of the device. Consideration for unprocessed platter regions, as would be found due to actuator arm shadow, or other sources of attenuation should be validated.

As the device processed by degaussing will not be mechanically and in some cases electrically operational, the validation by a lab is truly the only effective means to determine the effectiveness of the process on specific device models. Considering that the composition of hard drive products can vary from vendor, model or revision, each product to be degaussed should be verified in the lab before the service provider can deliver surety to the client that their process is effective.

**SECURE ERASE** Secure Erase was developed at the request of a consortium of drive manufacturers, and government departments. The project proposed was the creation of a protocol that could be developed into a standard for data destruction. This protocol was developed by the CMRR as an embedded technology that has been employed in the production of ATA / IDE devices as early as 1999 and adopted as a standard for SATA/ATA/IDE technology since 2002. As a standard based embedded technology, all SATA/ATA/IDE devices now support Secure Erase as part of their controller code, and all devices can be processed using a standard launch / control protocol. Employing privileged controller functions, Secure Erase has the ability to purge data on storage devices more efficiently than any externally controlled overwrite process. Achieving purge rates varying between as little as 17 minutes per 100 Gig, through to 41 minutes per 100 Gig, Secure Erase not only provides a contact based purge process, but the process has been certified time and again in laboratory evaluations to be effectively devoid of any data artifacts in all user accessible drive regions, including bad tracks or sectors. Achieving proven results, Secure Erase affords clients better piece of mind than the uncertainty provided by physical destruction methods. Additionally, the Secure Erase can be conducted on site using portable Secure Erase hardware such as the Ensonce Data Technology Inc. Digital Shredder, and the processed storage device remains a usable asset that can be re-deployed.

As a green technology, Secure Erase affords the end user no loss of their asset, no generation of e-waste, absolute care, custody and control of their assets, all this being delivered using a proven standards based technology.

We respect the fact that many data destruction policies are still employing outdated physical destruction processes, and feel that Secure Erase can play a very important role in improving the process by mitigating significant liability these policies impose. Considering that many companies do not have localized data destruction facilities at each office, many employ the practice of handing off storage devices for delivery to either company owned or service provider destruction facilities. The moment that a digital asset leaves the threshold of your offices, devices containing recoverable data are in the hands of those that can be considered strangers, regardless of any contract or assurances of confidentiality offered by any carrier or service provider. The vulnerability of loss by third party should be a very serious consideration for any CSO or CISO who is responsible for assuring that confidential information remains in the organization.

By using the Digital Shredder at the local premises before handing off storage device to a carrier, assures the organization that the vulnerability of exposure of confidential information is mitigated.



## Digital Shredder vs. Software Overwrites

There are **three major areas** that separate software overwrite from Secure Erase. Each area has a very obvious and meaningful advantage:

The first, and most important, is **compliance**: The US Guidelines for Media Sanitization is the document that serves as the benchmark for hard drive sanitization methodologies in the United States. You hear the term DoD 5220 thrown around fairly often, and it is a document that is extremely abused by the software companies. DoD 5220 has not recommended overwriting, or any hard drive sanitization methodology since the 1994 revision. Every version of DoD 5220 since that year makes no mention of hard drive erasure methodologies.

The only national guideline is NIST SP 800-88. Please see the Digital Shredder Sales Guide (page 23) for more information. You will find it rates different sanitization procedures. It clearly calls software overwriting a "clearing" methodology, while secure erase is rated as a "purge" of information. What does this mean? The NSA and NIST define clearing only secure up to the degree that the data may not be reconstructed using normal system capabilities, i.e., through the keyboard. The NSA and NIST define purging as rendering the data secure to the degree that the data may not be reconstructed through open-ended laboratory techniques. The Guidelines go on to call secure erase the best option for an organization when it is available. This clearly represents that the Guidelines for Media Sanitization in the United States recommend secure erase over any overwrite procedure.

In Canada, the guidelines are the RCMP's B2-001.

In Australia, it is the Australian Government's DoD ACS133.

Without the benefit of fully understanding the EU's standards, the facts remain the same – Secure Erase is a higher standard than any software overwrite. It is also a global hard drive manufacturer standard now embedded in the firmware of hard drives.

The next major factor is the **execution**: Secure erase is inherently more effective than any overwrite ever will be because of its very nature: it is executed from the firmware of the drive. Because of this, secure erase can deal with "bad sectors" that processes executed from BIOS and OS levels such as overwriting utilities cannot ever address. Firmware executed procedures are also impossible to interrupt externally. Ultimately, these, among other factors, are the reasons it is recommended above overwriting in NIST SP 800-88.

The final major factor is **speed**: Because secure erase is executed from the firmware, it is not limited by processor or BUS speeds, or by the drive interface. It can execute a full secure erase on a drive in 1/18th the time it takes to perform a less effective 7 pass overwrite. In fact, when compared to even a single pass overwrite, it is still usually more than twice as fast. When you consider the five critical requirements for a failsafe sanitization strategy:

1. Destroy data beyond forensic reconstruction – Software does not:
2. Ensure absolute care, custody and control of the process – Software does not:
3. Provide certification feature with a defensible audit trail – Software does not:
4. Process is scalable and easy to implement – Software is not:
5. Provide a green solution, reformat & image drive for potential reuse:

The Digital Shredder becomes the obvious solution.

For More Info

Click Here --->



<http://www.monomachines.com/Digital-Data-Destruction/HSM-DS-200-Digital-Shredder.htm>

## Data Loss Prevention: Managing the Final Stage of the Data Life Cycle Model

A Perspective on Decommissioning Storage Technology

For More Info

Click Here ---->



Perspective of a Reseller:  
By Ryk Edelstein  
Director of Operations  
Converge Net Inc.

May 2007

## Executive Summary

From the moment information is created until the end of its usable life, we, as custodians of this data, are responsible for ensuring it is secure. Where best practice had once dictated the means by which this data was protected, we have seen that due to inconsistencies in establishing a reliable protection model, best practice has gone the way of industry and legislative compliance obligations. What had once been career limiting and publicly embarrassing data security breaches, have now evolved to laws and punitive actions that can result in heavy fines, the incarceration of directors, serious public embarrassment, and the potential for the loss of the right of the organization to process credit card payments (in the case of PCI).

As we address the issues concerning the development of a compliance posture specific to the legislative or industry regulations that are applicable to our respective industries or activities, it is common to find that the policies developed focus on the lifecycle of the information from its creation, to storage, through to its transport over public and private networks. Frequently the final stage of our roles as custodians of this data is addressed with a simple statement about decommissioning these storage devices.

It is clear that the reason for the lack of a comprehensive decommissioning policy is due to the confusion over what the standards are and the availability of a truly effective solution suitable to both public and private sectors.

In this document, we look at the issues and technologies surrounding the proper decommissioning of end-of-life storage devices and how you can add government-recognized, data sanitization technology to your Data Loss Prevention model.

Don't let digital assets leave your control. Establish accountability and policy compliance. Take back your right to Care, Custody and Control™ with a proven technology capable of providing effective and efficient destruction of sensitive information in-house: *Secure Erase*.

For More Info

Click Here --->



For More Info

Click Here --->



## Table of Contents

**EXECUTIVE SUMMARY ..... 2**

**INTRODUCTION ..... 4**

**THE VULNERABILITY OF LEGACY DATA..... 5**

    SOFTWARE OVERWRITE ..... 5

    DEGAUSSING ..... 6

    PHYSICAL DESTRUCTION..... 7

**ENCRYPTION – PERCEPTION VS. REALITY..... 8**

**DRIVE DECOMMISSIONING, A NEED IN SEARCH OF A SOLUTION..... 9**

**LEVERAGING THE VALUE OF SECURE ERASE ..... 10**

    TAKING BACK YOUR RIGHT TO CARE, CUSTODY AND CONTROL™ ..... 10

    A RECOGNIZED SOLUTION..... 11

    AN ESSENTIAL COMPONENT IN ESTABLISHING COMPREHENSIVE COMPLIANCE..... 11

**SUMMARY ..... 12**

**ABOUT THE AUTHOR..... 13**

**CONTACT INFORMATION ..... 14**



## Introduction

Compliance, Best Practice or Policy: From the moment digital information is created, an organization inherits stewardship of this data and must ensure that the storage, transmission and access to this information are secure. From rights management that restricts data access, to the security of data at rest, or in transit over a private or public network, protection of sensitive data is paramount in order to minimize an organization's liability. Taking the protection of data beyond most established policies for data at rest and data in motion, our responsibilities extend to the destruction of the data on legacy storage devices that have reached the end of their useable life.

Legislative and industry compliance requirements aside, the need for the secure management of data throughout its lifecycle stems from best practice, and the responsibility for protecting confidential information rests with all parties that use or manage information technology assets. When one considers the diversity of various IT environments, current compliance requirements can not offer specific solutions, methods, or technologies; they only identify the desired net result, and penalties for failure to meet compliance.

When developing deliverables as part of a compliance mandate, it is essential that the business model effectively address the risks and vulnerabilities specific to the types of storage environment where the data resides. Typically, a compliance model would include the creation of policies specific to the protection of data in all modes. However, often these deliverables make little provision for the decommissioning of storage devices that have reached the end of their operational life. It is the responsibility of an organization to develop and enforce an accountable security policy protecting these storage devices, including the prompt disposal of their contents in a manner that ensures that at no point in the decommissioning process the devices ever pose additional risk and liability due to the loss of Care, Custody and Control™ of the storage devices.

The legacy data remaining on hard drives removed from workstations, servers, and storage systems poses significant data security vulnerability. Penalties for failure to properly eliminate user data from these storage devices can expose public or private parties to significant fines and incarceration (HIPAA, FACTA, Sarbanes-Oxley, Gramm-Leach-Bliley and PCI Data Security Standard among others), not to mention negative public exposure.

After extensive discussions with law enforcement, corporate and public sector IT and information security directors, service providers, and technology vendors, it is clear that there is significant confusion and concern about the lack of reliable data destruction technologies and services currently available on the market. Although there are service providers offering storage device destruction services, and software vendors claiming assured data sanitization, these options fail to deliver the care, custody and audited control necessary to efficiently and effectively comply with data destruction requirements. In many cases, these apparent solutions fail to deliver the level of protection that is expected by the consumer. To date, the only technology that effectively and reliably can assure that all objectives are met, and that no legacy data is going out the door is *Secure Erase*<sup>1</sup>.

---

<sup>1</sup> Tutorial on Disk Drive Data Sanitization, Center for Magnetic Recording Research, University of California San Diego, Dr. Gordon Hughes, April 17, 2007.



## The Vulnerability of Legacy Data

The growing concern over the presence of legacy data on retired hard drives, and the lack of suitable technology to effectively erase this data has led many organizations to warehouse their retired storage devices in order to mitigate risk that improperly decommissioned storage devices may pose. Despite the desire to dispose of, or return these end-of-lease units intact, the risk posed by anything less than certified data destruction is too great to allow these devices off the premises. Accumulated storage devices pose additional challenges specific to inventory control, classification and the potential risk that the loss of a single device can impose. As inventories grow while waiting for a reliable solution, the storage issue will typically reach a tipping point where the cost and effort of storing the devices will lead to the desire to get rid of these devices, and a potentially less-than-best practice of disposal being employed. These actions could include the allocation of a resource to process each drive using a software overwrite program (an investment of up to a couple days per device, and proven in most cases to leave recoverable data on the device); or the devices are shipped to an external service provider for destruction. Unless accompanied by a company employee or agent, to ensure the security of the devices through to the destruction stage, the organization loses its Care, Custody and Control™ of the assets once they leave the premises. Clearly, for those seeking an in-house means to effectively destroy legacy data at the time of decommissioning; these methods are not a viable solution.

Until fairly recently, the methods commonly used to destroy legacy information on hard drives included:

### **Software Overwrite**

Many software vendors state claims of DOD 5220 compliance when selling their software, but while they may be compliant, this standard is no longer considered a valid option for device decommissioning, at least not by the US government. Deemed by many in the field to be 10 years out of date, a DOD 5220 process can take over a day to process current drive storage capacities. And, the licensing-related cost to install and legally operate many of these software-based products is high when processing the quantities of devices commonly decommissioned at even a small or medium-sized business. Other shortcomings of the software overwrite approach include the lack of a defensible audit log, assured destruction of protected areas of the drive, and the lack of issuance of a destruction certificate that can be affixed to the device.

A significant concern specific to software based overwrite technology is the fact that the embedded controller on the hard drive is engineered to manage the data read/write process. The identification of bad sectors or tracks is managed by the controller whereby it can detect and rectify a failed write-cycle, re-allocate the data from a bad sector or track to an alternate location on the drive, then mark and segregate the original location as a bad sector or track. Once the track is marked as bad, the operating system and BIOS of the host no longer has the ability to access these segregated areas.

Consequently, during an attempted write-cycle, data that had been written to these bad sectors, remain throughout the software overwrite process. Typically there is little concern over bad sectors, except that in the segregation process, the data originally written to the sector or track is not erased and will remain in a recoverable or semi recoverable state. This concern is supported by comparative studies that have shown that many software overwrite products fail or halt when subjected to a bad sector or track during the overwrite process.

## ***Degaussing***

This process was initially designed for the destruction of non-rigid disks, and magnetic tape media. Degaussing involves exposing a device to a strong magnetic field capable of attaining the coercivity, or magnetic strength, of the storage media being erased; in effect re-polarizing the magnetic media and effectively erasing the stored data. As a byproduct of this operation, electromagnetic radiation produced during the degaussing process can interfere with nearby electronic and data processing equipment; and, the potential health concerns associated with the process requires that it either be conducted off-site or in an isolated environment.

The issues concerning the adoption of degaussing as a means to decommission hard drives include:

### **Power Required to Attain Effective Coercivity**

- The magnetic energy required to repolarize the platters of current high density hard-drive platter chemistry can be delivered by available degaussing devices capable of attaining better than 8,000 oerstead (or ampere-turns/cm), Older, lower-powered degaussing devices would not be effective in erasing data on hard drives composed of high-density platters<sup>2</sup>.

### **Effectiveness**

- Exposing a hard drive to magnetic energy as a means to destroy data has questionable effectiveness. This is due to the fact that the degaussing device will typically damage the spindle and rotor magnetics, often before destroying the data on the platter. With the drive electronics disabled, a user is unable to easily validate whether the platter, in fact, has been erased of recoverable data. Furthermore, components of the drive containing iron-based alloys can shunt magnetic energy away from the platters, thereby reducing the exposure of magnetic energy to proximate or shadowed regions of the platter.

### **Accountability**

- As a connection free process, degaussing provides no automated audit log, or certification that the device is effectively wiped of data. The only assurance offered is that the device had been placed in a degausser for a specified period of time. If the degaussing device were out of calibration and not providing the power levels necessary to destroy data, this would not be known until the next scheduled maintenance of the degaussing unit. Any processed hard drives would not have been effectively decommissioned, posing a significant risk for the client having the hard drives degaussed. At the completion of a degaussing cycle there is no way to ensure that the platter does not contain any recoverable data, short of dismantling the device and placing the platter on a spin stand in a laboratory.

---

<sup>2</sup> Tutorial on Disk Drive Data Sanitization, Center for Magnetic Recording Research, University of California San Diego, Dr. Gordon Hughes, April 17, 2007.

## **Physical Destruction**

Physical destruction offers a very wide range of possible interpretations. Many professional industrial shredding service providers employ their own proprietary technology to reduce hard drives to small particles. Some companies, not wishing to contract professional shredding services, have employed a variety of techniques, many of questionable merit, ranging from using a 20-ton press or a sledgehammer to the dismantling of the device and belt sanding the extracted platters.

The physical destruction of the hard drives is normally not carried out in-house and requires the transportation of the assets to the service providers' facilities. Having unprotected data leave the premises without any level of data destruction involves a loss of custody that exceeds the risk levels most Chief Security Officers might deem acceptable.

As a means to mitigate the risk of off-site destruction, many organizations employing out-sourced, physical destruction options require the assets to be accompanied by a company employee who is responsible for overseeing the entire destruction process, which should include a clearly-defined policy structured to minimize risk and confirms that the device has been destroyed beyond forensic reconstruction.

According to recommendations by the Center for Magnetic Recording Research (CMRR), and the National Institute for Science and Technology (NIST) recommendation 800-88, absolute destruction is accomplished when a particle is no longer large enough to contain a single 512kb record block. Based upon current platter chemistry this fragment would measure less than 1/125 of an inch<sup>3</sup>. This measurement is expected to be reduced further with the advent of higher-capacity platter chemistry, and other recording technologies such as perpendicular recording, and heat-aided coercion technologies.

The environmental impact caused by the waste generated as a byproduct of the physical destruction of millions of hard drives dumped each year accounts for a very significant environmental impact to not just the landfills many end up in. The composition of a hard drive reveals an array of metals and chemicals that warrant disposal in environmentally protected landfill sites, or the separation of components into a state where they can be responsibly recycled<sup>4</sup>.

With a growing adoption of "green" policies, and environmental stewardship programs, we are seeing many corporations and the public sector favoring green solutions over other such less environmentally sound options.

For More Info

Click Here --->



<sup>3</sup> *CMRR Protocols for Disk Drive Secure Erase*, Center for Magnetic Recording Research, University of California San Diego, Dr. Gordon Hughes, August 10, 2004.

<sup>4</sup> *Creating World Standards For Recycling And Harvesting Electronic Components*, Science Daily, <http://www.sciencedaily.com/releases/2007/03/070319175834.htm>, March 26, 2007.

## Encryption – Perception vs. Reality

Without a doubt, encryption is a very valuable technology for the protection of active data, and no policy would be complete without the proper application of encryption technology. Encryption, second to authentication, establishes protection and policy by which information can be accessed. The most common applications of encryption include the protection for:

### Information in Transit

- Information in transit over public (un-trusted) networks is commonly protected by encrypting each packet with triple-pass, DES encryption.

### Data at Rest in Storage Environments

- Whether server volumes, databases, client information, financial data, or other sensitive information, storage-based encryption solutions provide active protection of frequently accessed live data, while ensuring that unauthorized access is prohibited.

### Mail, File, and Data Encryption

- Data flowing over public or private networks are vulnerable to interception using easily accessible software tools and a bit of know-how. The need to communicate information securely over public networks to recipients who do not have a tunneled, VPN connection to the host network is achieved through the encryption of the message, file or data being transmitted using public key technology.

### Whole Disk Encryption

- In conducting our day-to-day business the need to transport sensitive data on portable computers, or the need to assure protection from unauthorized access on office or home PC's, warrants the implementation of whole disk encryption. Whole disk encryption protects active storage devices by requiring a valid pass-phrase upon access of the protected device.

Although encryption is a good means of protecting active data, the mechanics of encryption facilitate the access of secure information to any party providing the proper credentials. Typically the credentials required for the decryption of whole disk protection will be a pass-phrase entered by the user. Considering that most pass-phrases and passwords are typically less than 14 characters, and are composed on mnemonics, words or numbers that have meaning and can be remembered, the possibility to access whole disk encrypted storage devices remains a reasonable possibility. Add to this the fact that the effort that one will make to access protected information is proportional to the value of that information, then it is plausible that it is not necessarily the weakness of the technology, but the weakness of the pass-phrase that exposes the vulnerability of disk encrypted data.

As it is a technology designed for the protection of active data, encryption is not a valid option to decommissioning legacy data. A reliable and effective decommissioning technology should be applied to ensure that end-of-life devices are properly decommissioned, whether the contents are encrypted or not.

For More Info

Click Here --->



For More Info

Click Here --->



## Drive Decommissioning, A Need in Search of a Solution.

At the recent conference of the National Association for Information Destruction, many working sessions focused on the growing need for the responsible decommissioning of digital assets, and the establishment of best practices in this area. It was clearly evident that both the market place and service providers are seeking an effective solution.

The in-house practice of physical destruction of data storage devices by degaussing, disintegration, shredding, or other means is not only hazardous, but currently has limited effectiveness, and unacceptable audit controls. Contracting external service providers, meanwhile, exposes the organization to the loss of Care, Custody and Control™ of their assets. It also offers no automated audit control and could expose the client to significant additional costs.

Recognizing the need for reliable, on-site hard drive decommissioning, EDT took on the challenge of developing a product that would address the challenges faced by both public and private sector markets. The technology developed had to be capable of reliable device decommissioning of all recordable areas. It had to be more efficient in processing the hard drive than other technologies. It had to automatically maintain an audit log and it had to be operational on the client's site.

Initial efforts led The Company's design team to focus on the development of a software-based solution using the *Secure Erase* standard as designed by the University of California San Diego's Center for Recorded Magnetic Media. *Secure Erase* provided an industry recognized technology delivering the level of data destruction that The Company needed to create a marketable product. Unfortunately, the power of *Secure Erase* also posed a significant threat if exploited by virus, crimeware, or malware developers, as the hard drive could be rendered void of any recoverable data. Before *Secure Erase* could be adopted by software vendors looking to market an industry recognized and developed data sanitization solution, BIOS, and Operating System vendors incorporated features in their products that would intercept and inhibit the application the *Secure Erase* process on the hard drive<sup>5</sup>.

Faced with the challenges specific to developing a software solution, it became evident to The Company's design team that the best approach was to create a portable, stand-alone *Secure Erase* appliance to effectively destroy data beyond forensic reconstruction. Not having the constraints imposed by a diverse variety of hardware platforms, the company captured the opportunity to design an appliance from the ground up. Suitable for military or office use, the *Dead on Demand™ Digital Shredder™™* features a three-bay design, and is the only *Secure Erase* appliance on the market capable of decommissioning IDE, ATA, SATA, and SCSI devices.

Faster and more effective than any overwrite technology, the *Dead On Demand™* appliance processes hard drives in an eighth of the time required by competing overwrite products using a DOD 5220-M process. The *Dead on Demand™ Digital Shredder™™* identifies each device inserted, and automatically logs the hard drive's manufacturer, the model and serial number, the operator's name and the date. Once the process is successfully completed, the appliance logs the procedure(s) employed on the drive as well as the elapsed time. All of this information is then compiled to provide a certification record for the hard drive. Each certification record is stored in an internal audit log that can be exported. Additionally, *The Digital Shredder™™* will issue an adhesive destruction certificate to be placed on the drive.

---

<sup>5</sup> DAMAGE CONTROL, Search CIO.com, [http://storagemagazine.techtarget.com/magItem/0,291266,sid19\\_gci1218700\\_idx5,00.html](http://storagemagazine.techtarget.com/magItem/0,291266,sid19_gci1218700_idx5,00.html), John Sterlicchi, 2006.

For More Info

Click Here --->



Unlike physical destruction methods, the *Dead on Demand™ Digital Shredder™™* virtually ‘shreds’ data, and offers a truly “green” solution that delivers 100 percent data loss that rival physical destruction methods. Yet, unlike physical destruction, devices processed by the *Dead on Demand™* appliance are returned to a state where they can be redeployed. As a final stage of the decommissioning process, *The Digital Shredder™™* provides the operator with the capability to select the choice of file system formats to be placed on the processed device. The operator can also apply a standardized image, if desired.

The effectiveness of the *Dead on Demand™* device has been recognized by government, crime laboratories and forensics specialists for its exceptional ability to eliminate all traces of legacy data on all accessible areas of the subject drive<sup>6</sup>. This assurance of media purity is of critical importance when processing subject devices for forensic audit, as any trace of legacy data -- even data which is present on a new hard drive as a byproduct of the calibration stages of manufacturing -- can violate the integrity and acceptance of the information collected from the work-drive used for analysis.

## Leveraging the Value of Secure Erase

As both the public and private sector move closer to establishing data privacy compliance levels, the need to address the decommissioning of end-of-life storage technology is a very intrinsic part of any compliance model. Any security or compliance policy lacking a solution capable of delivering the effectiveness of the *Dead on Demand™* product is in fact incomplete.

*Secure Erase*, as applied with the *Dead on Demand™ Digital Shredder™™*, provides both the public and private sector with a very cost-effective appliance that enables them to eliminate inventories of retired hard drives and rapidly decommission end-of-life or end-of-lease computer work-stations, servers, storage arrays and intelligent printers in-house. The ease of use, efficiency and effectiveness of the *Dead on Demand™ Digital Shredder™™* provides a high-value solution for any organization.

## Taking back your right to Care, Custody and Control™

The risk in sending out hard drives for destruction by an external supplier is significant enough to require that these assets be accompanied through every step of the process. And considering the results, any company currently using this method may wish to seriously consider whether the process used, or the size of the platter particles produced, ensure that no data is recoverable. The upstream liability to the organization also should be evaluated to determine if there is any concern about the service provider’s ability to dispose of the decommissioned byproduct in an ecologically approved manner. This assessment should include any potential negative impact on the client’s public image.

The exposure to the significant risks of employing less-than-reliable software solutions, or the loss of Care, Custody and Control™ resulting from sending digital assets out for external decommissioning, is reason enough for any organization to establish an in-house decommissioning infrastructure. The *Dead on Demand™ Digital Shredder™* provides a solution that delivers the full Care, Custody and Control™ necessary to ensure policy compliance and the peace of mind that the hard drive decommissioning process has been conducted effectively. Adding *The Digital Shredder™* to the arsenal of security

---

<sup>6</sup> Data Shredder Data Recovery Test Report, Detective Michael Leclair, July 29, 2006.

technologies necessary to protect this information will ensure that no end-of-life device will ever leave the premises without 100 percent data loss.

### **A recognized solution**

Approved by the Center for Recorded Magnetic Media at University of California San Diego, the National Institute for Science and Technology (NIST) in their recommendation 800-88, the Canadian Government<sup>7</sup>, and many companies for the effective implementation of *Secure Erase*, the *Dead on Demand™ Digital Shredder™* is quickly earning market acceptance, as well as receiving growing public awareness.

The NIST recommendation 800-88 states that second to effective physical destruction, *Secure Erase* is the single best solution as a responsible and effective means to decommission end of life hard drives. The NIST recommendations are based upon research collected from within the US government, including military, security, administration, and technical agencies, as well as from academic and research sources. The aim of this research is to establish a best practice model for consideration by other parts of the public and private sector in the development of their policies.

### **An Essential component in establishing comprehensive compliance**

Much has been written about the technologies and services available to decommission hard drives. Most of this has been prepared by manufacturers touting the merits of their products; others have been composed of practices employed by enterprise and service providers in an effort to attain a level of information security. Some of the techniques offered include using sledgehammers, or using kilns to render a drive into metallic slurry, or using nail guns for purposes for which they were never intended. Many of these solutions do not deliver a method that can be deemed acceptable to policy in either the public or private sectors.

When looking to define the final chapter in your data lifecycle management model, it is essential to adopt a solution that will ensure that there will be no data leakage during the decommissioning process. The risks to an organization imposed by law or industry regulation, including the damage to public image, are far too significant to ignore and are now truly within reach. The development of policy should reference reliable sources for acceptable standards, such as those found in the NIST 800-88 recommendation, and from other recognized authorities. Whatever decommissioning alternative you are considering, assess whether these alternatives provide the assured data destruction level as specified by your policy and the laws and regulations for your industry. Then determine whether these solutions address your needs for Care, Custody and Control™, as well as meet your requirement for an exportable and defensible audit log, the issuance of certificates, and a portable on-site solution.

For More Info  
Click Here ---> 

<sup>7</sup> Suggested DSX Replacement Products, <http://www.rcmp-grc.gc.ca/tsb/pubs>, March 2006.

## Summary

From the moment that information is created to the end of its usable life, we are accountable as custodians for ensuring that this information is secure. To date less than 20 percent of all merchants have exhibited compliance to PCI, and even fewer meet with legislative compliance, such as Sarbanes-Oxley. Although these organizations are not yet compliant, they will need to become compliant in the near future.

With the increasing prevalence of reports of data loss, not a week goes by without someone making the headlines for their loss of confidential or sensitive information. The tolerance for these incidents will drive industry regulators, and those enforcing penalties for failure to comply with privacy laws, to add more teeth to their compliance regulations.

As penalties are assessed, and corporate directors face legal action for their failure to meet compliance objectives, we will witness the push to better secure sensitive information increase from the moderate need we see in the marketplace at present. And, as this market need grows, so will the demand for the technologies necessary to meet the objectives.

With increased focus on risk and vulnerability assessment tools, data loss prevention technology, encryption, application firewalls, and enhanced zone and perimeter security, the need to address the decommissioning of stored digital assets on end-of-life hard drives will increase proportionally. The business values that *Secure Erase* addresses may offer the most significant peace of mind and value over any other technology.

A responsible cradle-to-grave compliance model is not a complete solution if you are not addressing a responsible decommissioning policy.

For More Info

Click Here ---->



## About the Author

Ryk Edelstein, is the director of operations for Converge Net Inc, a Montreal based Enterprise Security and network Infrastructure VAR. With more than 25 years experience in developing, analyzing and securing networks for numerous large to mid-sized enterprises, Ryk has guided his companies through years of continued success by listening to client needs and aligning technology with business values.

Trained as a specialist in Tactical Surveillance Counter Measures, Ryk understands the importance of the security of information, and the methodologies and technology necessary to secure communications streams. As an instructor on Information Security at the York University's Schulich School of Business, Ryk has instructed many public and private sector directors and managers in the elements of communication security and on how to establish best communications practice.

Focusing at the lower layers of the network model, Converge Net specializes in addressing network conditions from the Packet Level up. As a solution-driven company, Converge Net partners with vendors to help clients realize management, network performance, security and compliance objectives. As a VAR for McAfee, Vontu, PGP, Network General, Packeteer, Acunetix, Cisco, Destruct Data and EDT, Converge Net leverages strategic vendor technologies to deliver a comprehensive solution model.

For More Info

Click Here --->



550 Sherbrooke St. West  
West Tower Suite 250  
Montreal, Quebec H3A 1B9  
www.converge-net.com

## Contact Information

HSM GmbH + Co. KG  
Bahnhofstrasse 115  
88682 Salem / Germany

Tel. +49 (0) 75 53 / 822 - 0  
Fax +49 (0) 75 53 / 822 - 160

info@hsm.eu  
www.hsm.eu

www.digital-shredder.com

For More Info

Click Here --->

