

Best Security Practice for
DATA MEDIA SANITIZATION AND DESTRUCTION

PUBLISHED BY THE OFFICE OF INFORMATION TECHNOLOGY – CANUARY 2008

"BEST PRACTICES ARE THE PROCESSES AND ACTIVITIES THAT HAVE BEEN SHOWN TO BE THE MOST EFFECTIVE"

BEST SECURITY PRACTICE (BSP) No. 8: ALL UNLV IT SYSTEMS OWNERS AND MANAGERS SHOULD ESTABLISH AND MAINTAIN A BASELINE INFORMATION SECURITY STANDARD FOR THE TERMINAL OR FINAL PROTECTION OF CRITICAL, PRIVACY, OR SENSITIVE DATA AT REST IN VARIOUS FORMS OF MEDIA.

OBJECTIVES: To provide direction and support for information security in accordance with internationally accepted standards (ISO 17799/27001), business requirements and relevant State and Federal laws and regulations. This technical Best Practice directly supports the UNLV Capstone Policy IS01 - Information Security for Information Resources and Asset, and defines the acceptable use of UNLV information technology services and accounts. **This Best Practice is also mandated under UNLV Data Media Sanitization and Destruction Policy (IST406).**

BACKGROUND: UNLV's information security best practices initiative is to prevent and minimize sensitive data loss or compromises. Dependencies on technology to support business functions and delivery of UNLV programs potentially expose the University to risks of accidental and intentional data loss by failing to properly dispose of data and data media at the end of its life-cycle.

The purpose of this Practice is to:

- Establish the protection against inadvertent loss or breach of sensitive information from lack of proper information destruction.
- Establish a standard for data media sanitization and destruction.

In order to manage information security comprehensively, this Best Practice serves the to:

- Establish the practice that every UNLV information technology (IT) online or offline storage device that has had UNLV information stored on it must be properly and securely sanitized or destroyed prior to disposal or reassignment.
- Require organizations to identify those devices that contain UNLV information.
- Delineate specific technical methodologies for the secure processing and destruction of the UNLV information.
- Delineate specific responsibilities for the secure processing and destruction of the UNLV information.
- Establish standards for addressing security consistency.

AUDIT CONTROL: Security audits will inspect the in-use security applications, procedures, and processes of passwords by using this Best Practice, including timeliness of updates, for compliance to security best practice standards. This Best Practice will be audited using the appropriate BS 7799.2:200x Audit Check List, dated 8.08.2005 or later, and through a complete review of all related complaints (security incidents) that occurred after the previous audit.

BEST PRACTICE STANDARDS (BSP)

INFORMATION SECURITY STANDARDS AND CONTROLS. The following are the Data Media Sanitization Best Practice Standards that should be applied to each IT storage device, as appropriate, to be in minimum compliance with UNLV standards.

BSP: 3--1 Disposal of Computers and Hard Drives. All UNLV computers and hard drives shall be returned to _____ for appropriate redeployment or other disposal processing.

Before any UNLV owned or managed hard disk or system containing a hard disk is transferred, surplus, or donated, it must be sanitized by reformatting the hard drive in a secure manner or by using an approved wipeout utility. Simply deleting a file is not sufficient to prevent someone from undeleting the file later. If the system will be donated to an outside organization, it should have either no operating system or the original operating system installed on it after sanitization.

Consult with your Unit Security Person prior to getting rid of any computer equipment to get assistance in properly performing the sanitizing task, and in obtaining an approved wipeout or formatting utility. The security person or their designee must sign a certification that the equipment has been properly sanitized before it can be surplus, transferred, or donated. The Unit Security Person should save copies of all certification statements.

Information on systems and hard disks sent outside of your organization for repair or data recovery should be protected from disclosure by contract with the company or organization performing the service.

BSP: 3--2 Sanitizing of Hard Drives. Sanitizing hard drives is the process of removing sensitive information from storage media in a manner that gives assurance that the information cannot be recovered by keyboard or laboratory attack. Before the sanitization process begins, the computer should be disconnected from any external network to prevent accidental damage to the network operating system (OS) or other files on the network. In addition, when possible, users should audit the sanitizing process to ensure data is no longer retrievable. This means a knowledgeable person should witness the sanitization process and verify that the hard drive was sanitized. *Please note: if the digital media device is non-operational or cannot be booted up, the device must be crushed, drilled, degaussed, or incinerated.*

The most common techniques for properly sanitizing hard drives include:

- 1. Physically destroying the drive, rendering it unusable.** Hard drives should be destroyed when they are defective or cannot be economically repaired or sanitized for reuse. As an added security measure, when practical, operable hard drives no longer deemed economically viable should be overwritten or degaussed prior to destruction. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive.
- 2. Degaussing the drive to randomize the magnetic domains – most likely rendering the drive unusable in the process.** Degaussing is a process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack.
- 3. Overwriting the drive's data so that it cannot be recovered.** Overwriting is an approved method for sanitization of hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) and zeros (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., "11111111" followed by "00000000") the magnetic fluxes will be physically changed and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge the hard drive, the UNLV requires overwriting with a pattern, and then its complement, and finally with another pattern. Sanitization is not complete until three overwrite passes and a verification pass is completed.

Currently the University of Nevada does not have a site license for sanitation tools. The following table shows a few examples of free and commercially available sanitation tools)

PROGRAM	COST	PLATFORM	COMMENTS
AutoClave staff.washington.edu/jdlarios/autoclave	Free	Self-booting PC disk	Writes just zeroes, DoD specs, or the Gutmann patterns. Very convenient and easy to use. Erases the entire disk including all slack and swap space.

CyberScrub www.cyberscrub.com	39.95	Windows	Erases files, folders, cookies, or an entire drive. Implements Gutmann patterns.
DataScrubber www.datadev.com/ds100.html	\$1,695	Windows, Unix	Handles SCSI remapping and swap area. Claims to be developed in collaboration with the US Air Force Information Welfare Center.
DataGone www.powerquest.com	\$90	Windows	Erases data from hard disks and removable media. Supports multiple overwriting patterns.
Eraser www.heidi.ie/eraser	Free	Windows	Erases directory metadata. Sanitizes Windows swap file when run from DOS. Sanitizes slack space by creating huge temporary files.
OnTrack DataEraser www.ontrack.com/dataeraser	\$30-\$500	Seif-booting PC disk	Erases partitions, directories, boot records, and so on. Includes DoD specs in professional version only.
SecureClean www.lat.com	\$49.95	Windows	Securely erases individual files, temporary files, slack space, and so on.
Unishred Pro www.accessdata.com	\$450	Unix and PC hardware	Understands some vendor-specific commands used for bad-block management on SCSI drives. Optionally verifies writes. Implements all relevant DoD standards and allows custom patterns.
Wipe wipe.sourceforge.net	Free	Linux	Uses Gutmann's erase patterns. Erases single files and accompanying metadata or entire disks.
WipeDrive www.accessdata.com	\$39.95	Bootable PC disk	Securely erases IDE and SCSI drives.
Wiperaser XP www.liveye.com/wiperaser	\$24.95	Windows	Erases cookies, history, cache, temporary files, and so on. Graphical user interface.

The process and forms required to surplus IT items at the UNLV are available at [_____](#).

BSP: 3--3 Sanitization of Portable Media. Diskettes and other magnetic storage media that contain any UNLV academic or business data or software must be sanitized when they are no longer needed. Portable media may be reused after overwriting or degaussing, or they may be destroyed. Simply deleting a file is not sufficient to prevent someone from undeleting the file later. If the system will be donated to an outside organization, it should have a complete operating system installed on it after sanitization.

Portable media (diskettes, tapes, CD-ROMs) may be destroyed by crushing, incinerating, shredding, or melting. If they are to be reused, portable media must be digitally erased or "wiped" using a secure erasure program like the Norton Utilities WIPEINFO before being reused by other parties. Programs other than WIPEINFO must be approved by the Information Systems Security Officer before being used. *Please note if the digital media device is non-operational or cannot be booted up, the device must be crushed, drilled, degaussed, or incinerated.*