

Office of Operations Review and Audit



Program Review

**UW Procedures and Methods
for Removing Data from Surplus Computers**

January 2005

Table of Contents

	Page
Scope	1
Background	1
Discussion	2
Data Removal	3
Effective Removal Methods	3
Less Secure Removal Methods	4
Computer Surplus Procedures	6
Conclusion and Recommendations	8
Appendices	9

SCOPE

The University of Wisconsin System Office of Operations Review and Audit reviewed University of Wisconsin (UW) System institutions' procedures and methods for removing data from the hard drives of surplus personal computers at the time of disposal. During the review, we conducted telephone interviews with staff at all UW System institutions responsible for computer surplus equipment. UW staff we interviewed included surplus managers, directors of information technology services, and campus network support staff. We also reviewed the procedures of some other higher education institutions.

The review was limited to desk analysis of disposal procedures and methods. No computers were actually checked, with the exception of those examined by UW-Madison audit staff as part of a separate review. Also, the review focused on disposal procedures, rather than on procedures for safeguarding stored confidential information in the regular course of business.

BACKGROUND

This review was prompted largely by the concerns raised in various studies, analyses, publications, and news media. For instance:

- The *Chronicle of Higher Education* reported on February 14, 2003 that two researchers at the Massachusetts Institute of Technology found recoverable information from some computer hard drives they purchased from eBay. The recoverable information included corporate personnel memos, love letters, credit card numbers, and ATM transaction accounts and histories.
- *CNN.com* reported on February 13, 2003 that a State of Kentucky computer put up for sale as surplus contained confidential files of thousands of people with Acquired Immunodeficiency Syndrome (AIDS) and other sexually transmitted diseases.
- *Federal Computer Week* reported on August 26, 2002 that the U.S. Department of Veterans Affairs has had to tighten its policy on the disposal of old computers after some computers containing sensitive personal information about veterans, including medical records, were given away.

**Sensitive information was left
on some surplus computers.**

In 2003 the University of Iowa and University of Michigan conducted internal reviews of their property disposition practices. The University of Iowa Internal Audit Department reviewed the surplus computer disposal practices at the University of Iowa College of Medicine. The audit staff recovered data of a sensitive nature from two of the three computers selected among the 30 computers that were waiting to be sent to surplus.¹ Auditors at the University of Michigan

¹ The University of Iowa, Internal Audit Department. *UIHC/College of Medicine Review of Surplus Computer Disposal Practices*. May 23, 2003.

analyzed 28 computers that were waiting to be sold from more than a dozen departments. Nineteen computers still had university data on them, and five of these 19 computers contained sensitive information, including student names and identification numbers that contain Social Security numbers; employee names and Social Security numbers; staff home and cell phone numbers; and student applicants' names, addresses, telephone numbers, birth dates, and standardized test scores.²

DISCUSSION

According to the National Recycling Coalition, between 1997 and 2007, nearly 500 million personal computers will become obsolete -- almost two computers for each person in the United States.³ The UW System disposes of hundreds of personal computers each year. For instance, UW-Eau Claire, Green Bay, La Crosse, and Oshkosh each disposes of approximately 400 personal computers and UW-Madison sends about 300 tons of personal computer-related materials to recycling programs annually. UW System institutions generally replace their personal computers in three to four years, the typical useful lifespan of a personal computer.

Certain data the UW System stores on personal computers are subject to both state and federal privacy laws. A variety of personal information is protected, including:

- ***Student records:*** The federal Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. Generally schools may disclose, without consent, personally identifiable information from education records under certain specific circumstances. The schools may also disclose, without consent, "directory information", including a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, the schools must inform the students about directory information and allow the students a reasonable amount of time to request that the schools not disclose directory information about them.
- ***Financial information:*** The federal Gramm-Leach-Bliley Act (GLBA) requires all financial institutions (higher education institutions are considered financial institutions under the Act) to protect the security and confidentiality of personally identifiable financial information.
- ***Health information:*** The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule protects all individually identifiable health information. Individually identifiable health information includes many common identifiers, such as name, address, birth date, and Social Security number.

<p>A variety of personal information is protected by state and federal laws.</p>

² University of Michigan, Office of Financial Analysis. *Computer Disposal Process*. July 17, 2003.

³ National Recycling Coalition, "How to Properly Manage Your Old Electronic Equipment: A Guide for Consumers and Businesses." April 15, 2004. <<http://www.nrc-recycle.org/resources/electronics/managing.htm>>.

The protection of privacy and confidentiality spans numerous Wisconsin statutes. Even with a generous open records law, Wisconsin laws on privacy and records confidentiality call for appropriate protection and safeguards of confidential information, including computerized information. For example, s. 19.65, Wis. Stats., requires that a state agency having custody of records develop rules of conduct for employees who are involved in collecting, maintaining, using, providing access to, sharing or archiving personally identifiable information. UW System Board of Regents' Policy Document (RPD) 97-2, "Policy on Use of University Information Technology Resources," also calls for UW institutions to take reasonable precautions to protect electronic documents containing private and confidential information.

Failure to securely remove confidential data from used computers may be a violation of privacy laws if the confidential data is retrieved later by people who should not have access to the information. However, removing the data poses financial and technical challenges. This report describes the methods UW System institutions use to remove data from surplus personal computers and provides an overview of how UW institutions dispose of surplus computers.

DATA REMOVAL

Secure deletion of data stored in surplus computers is more complicated than it seems. When the data are saved on the computer's hard drive, the information is written as magnetic pulses on specific spaces on the hard drive. Contrary to public belief, deleting a file using the delete key and reformatting the hard drive does not necessarily remove the information from the hard drive.⁴ Furthermore, surplus computers are not always operable, or even if they are operable, the operating systems may be obsolete and there are few secure-file-removing software programs that would run on obsolete operating systems. We reviewed effective methods for removing data and also identified some less effective methods.

Effective Removal Methods

Data can be securely removed in a number of ways. Some of the most widely suggested methods include wiping, degaussing, and destruction. Our review found that UW institutions have used some of these commonly-used methods for removing data from surplus computers prior to disposal:

- ***Wiping***: Wiping refers to a process that writes data over the hard drive, such that any data stored on the drive are overwritten by the new data. In order to ensure that the stored data cannot be easily retrieved, the stored data area on the hard drive may have to be overwritten several times. A number of commercial disk-wiping utilities have been developed, including KillDisk, AutoClave, CyberScrub, Best Crypt Wipe, and Eraser. Wiping a hard drive can be time consuming depending on the speed and performance of the computers. UW-Madison, Stout, Superior,

Some UW System institutions use disk wiping utilities to wipe the hard drives of surplus computers.

⁴ Kinney, John. "Securely Deleting Files", December 12, 2000. <<http://www.sans.org/rr/privacy/deleting.php>>.

and UW Colleges dispose of their surplus computers through UW-Madison Surplus With A Purpose (SWAP), and SWAP uses KillDisk to wipe hard drives of surplus computers that are offered for resale and redistribution. UW-Milwaukee's College of Letters and Science uses SuperShredder to wipe hard drives. UW-Extension uses Boot and Nuke, a disk wiping utility, to wipe computer hard drives at the Pyle Center, Learning Innovations, and Wisconsin Public Radio and Wisconsin Public Television. UW-Stevens Point also uses a disk wiping utility software to overwrite hard drives.

- *Degaussing*: Degaussing is a process by which the hard drive is subjected to a powerful magnetic field. Data erasing is achieved by returning the hard drive to its neutral state. Degaussers are commonly used for tape media but will also work with most hard drives. Degaussing often destroys the hard drive's timing tracks and renders the drive inoperable. Thus, degaussing is the preferred method if the hard drive will not be used again. The UW-Milwaukee College of Letters and Science, UW-Platteville, and UW-Extension use degaussers to remove data from hard drives that cannot be wiped with disk wiping utility software.
- *Destruction*: A hard drive can be made inoperable by physical force, such as drilling holes, hammering, or mutilating. However, physical destruction does not erase the data; it simply makes the drive inoperable in a computer. The most cost-effective and environmentally sensitive method for destroying a hard drive is to use a disintegrator. UW institutions are not generally involved in the actual physical destruction of surplus computers that no longer have resale value; most of the computers without resale value are sent to the Wisconsin Department of Corrections for recycling. UW-Green Bay uses a hammer to make hard drives that were not part of a computer system inoperable.

Removing data that are stored in the surplus computer hard drives is largely the responsibility of campus or department information technology staff.

Less Secure Removal Methods

UW staff with whom we spoke had received no reports of instances in which UW confidential information had been inappropriately disclosed through surplus personal computers. While this is reassuring, our review identified some practices which may not securely remove UW data stored on computer hard drives at the time of disposal:

- *Reformatting*: Most operating systems, including Microsoft Windows, store information on the hard drive in two areas – system and data. The system area contains information about where on the hard drive (in which sectors) the data are stored. The data area contains the actual data or files. When a hard drive is reformatted, the operating system normally overwrites the system information but does not overwrite the data area.

Some UW institutions only reformat the hard drive at the time of disposal. Reformatting the hard drive appears to be adequate for surplus computers that are sent to SWAP for disposal, as SWAP uses KillDisk to wipe the hard drives prior to disposal. Reformatting also may be adequate for computers that are used in areas where confidential data storage is not an issue.

However, UW institution disposal procedures are not based on where the surplus computers have been used. Thus, the possibility exists that a computer that was used to store confidential information could be transferred to another university unit, resold, or donated with reformatting being performed only on the hard drive. Since the area on the hard drive where the data are stored is not overwritten during reformatting, the data could potentially be recovered.

Reformatting and ghosting the hard drives do not securely remove the stored data.

- *Ghosting*: Ghosting or disk imaging is the copying of the entire contents of a hard drive, including its configuration settings and applications, to another hard drive. Ghosting has proven to be an efficient method of loading configuration settings, operating systems, and applications to multiple machines. However, literature we reviewed on secure file removal does not include ghosting among the suggested secure data removal methods. Since ghosting occurs by overwriting the tracks on the hard drives, ghosting is most effective only if the host and target hard drives are of the same size. Thus, ghosting could potentially leave some tracks in the surplus computer hard drives untouched. A number of UW System institutions reported using ghosting prior to disposal.
- *Replacement*: Computer hard drives that have become defective but are still under warranty can be returned to the manufacturer for replacement. UW institutions have taken advantage of this service. When a hard drive fails, writing data to the drive or removing data from the drive may no longer be possible. However, the warranty can become void if UW staff attempt to repair the hard drive, unless the UW institution has received authorization from the manufacturers.

When hard drives are returned to the manufacturers, they typically refurbish the returned hard drives and sell them. UW staff we talked to indicated they don't have knowledge of the manufacturers' refurbishing process. We reviewed contract language from the UW System and state contracts for desktop and laptop computers. The state contracts include a provision to hold the UW System harmless from legal actions or claims resulting from the negligent performance by the vendors. However, the contracts do not address disclosure of confidential information resulting from the vendors' or manufacturers' failures to securely remove data from the returned hard drives prior to their being resold.

Recognizing that the returned defective hard drives may contain sensitive information that could be recovered, Dell offers its customers the Keep-Your-Hard-Drive service. The service allows the customers to receive a replacement hard drive but still keep the defective hard drive for proper disposal. The service is available at the time of purchase for a nominal fee. UW-La Crosse has purchased this service. UW-Green Bay is also considering purchasing this service for future personal computer orders.

Secure data removal may require additional labor, software, and hardware costs and can be time consuming. However, the benefits can easily outweigh the financial and other costs associated with having sensitive and confidential information recovered from surplus computers. Thus, *we recommend that UW System institutions: 1) securely remove data from surplus computers prior to disposal; and 2) consider purchasing a service similar to Dell's Keep-Your-Hard-*

Drive service, if such a service is available. Where such a service is not offered, we recommend that UW System Administration and UW System institutions include a provision in personal computer contracts to shield the UW System from potential liability resulting from inappropriate disclosure of confidential information through the vendors' or manufacturers' failure to securely remove data from hard drives the UW System institutions return for replacement.

COMPUTER SURPLUS PROCEDURES

Disposal of personal computers is regulated primarily by federal and state legislation on hazardous waste, as personal computers contain hazardous materials, including lead, mercury, and cadmium. We interviewed UW institution staff about procedures for disposing of surplus computers and reviewed procedures of other higher education institutions.

The procedures for disposing of surplus personal computers vary among UW institutions. This was expected, as UW institutions have different administrative structures and business practices. In addition to data removal, the institutions' procedures typically involve surplus declaration and disposition. First, UW institution units disposing of personal computers normally complete a surplus declaration form. Then, the surplus computers are picked up, evaluated, tagged, and stored until they are disposed of. At most UW System institutions, surplus computer disposal is a function of the procurement or purchasing office. At UW-Platteville, the College of Engineering is responsible for disposing of its own computers. UW-Madison, Stout, Superior, UW Colleges, and System Administration send most of their surplus computers to SWAP for disposal.

The Wisconsin Department of Administration (DOA) has promulgated rules for declaration and disposal of surplus materials and equipment. Chapter Admin 11, Wis. Admin. Code, specifies seven methods of disposal: 1) transfer or sale to another state agency; 2) transfer or sale to a municipality; 3) sale to the public; 4) trade-in on replacement equipment; 5) sale for salvage value; 6) scrapping; and 7) destruction. The DOA Procurement Manual prohibits donations of surplus property to private individuals, for-profit organizations, or state employees, as well as sale to state employees unless the items are sold at announced public sales or auctions. The methods UW institutions use to dispose of surplus computers appear to be consistent with DOA regulations and policies. UW institutions reported using the following methods of disposal:

UW System institutions use a variety of methods to dispose of surplus computers.

- ***Recycling:*** Some UW staff we interviewed indicated that anywhere between 75 to 90 percent of their institutions' surplus computer units ultimately end up in recycling, as they no longer meet the institutions' minimum standards or have no resale value at the time of disposal. Recycled computers are sent to UW or state-contracted recycling programs.
- ***Reuse:*** UW institutions typically have established some minimum standards for the reuse of personal computers. These standards differ among UW institutions. At UW-La Crosse, the personal computer must have at least a Pentium III processor to be reused. UW-River Falls

surpluses personal computers with a processor with a speed of less than 200 megahertz and a hard drive of less than three gigabytes. Computers that meet the minimum standards and are in working condition are reassigned for use elsewhere on campus if there is a need. A number of staff we interviewed indicated that because of their tight budget situations, the institutions keep the computers longer than the normal three to four years. As a result, few surplus computers meet the minimum standards for reuse when they are declared surplus.

- *Sale*: All UW institutions participate directly and indirectly in the sale of surplus computers. Most institutions sell the surplus computers directly to the public, while a few sell them through SWAP. The volume of surplus computers sold varies depending on how long the computers are kept and how much time and how many resources institutions devote to the sale.
- *Donation*: Some UW institutions donate their surplus computers directly to schools and other non-profit organizations. Some surplus computers that are not sold or donated are sent to the Wisconsin Department of Corrections for recycling. The Department of Corrections also donates these surplus computers to schools and non-profit organizations.

Institutional staff with whom we spoke indicated staff at their institutions are well aware of the risks associated with surplus computers. All UW System institutions reported having procedures for surplus computer disposal, although only UW-La Crosse, Madison, Milwaukee, Stevens Point, Stout, and Extension have adopted written policies or procedures. A review of these policies and procedures indicates that UW-La Crosse, Madison, Milwaukee, and Extension require the hard drive to be scrubbed or the data to be securely removed. (See Appendix 1 for UW-Extension's policy.) To reduce the possibility of the disposal of surplus computers before data are securely removed, ***we recommend that UW System institutions develop formal policies and procedures for disposing of surplus personal computers that include secure data removal methods.***

Some UW System institutions have developed formal policies and procedures for surplus computer disposal.

Our research shows that some other higher educational institutions have adopted formal computer disposal policies or procedures. The institutions whose policies or procedures we reviewed include Indiana University, the University of Michigan, the University of Minnesota, New York University, University of California-Berkeley, and the University of Washington. The Michigan, Minnesota and Washington policies and procedures require data to be securely removed from hard drives. The Washington procedure also requires a signed form certifying that data files have been destroyed. (See Appendix 2.)

The UW System does not currently have systemwide policies or procedures on surplus computer disposal. The UW System is not unique, as none of the university systems whose policies we examined have systemwide policies that address this. Some university systems have surplus-property policies, but they are not specific to surplus computers and do not address data removal. Nevertheless, the UW System could only benefit from increased systemwide awareness of the need for secure data disposal. One means of enhancing awareness would be to amend RPD 97-2,

on information technology resources, to address the secure destruction of private and confidential records prior to computer disposal.

CONCLUSION AND RECOMMENDATIONS

Our review found that all UW System institutions have procedures for disposing of surplus computers, and some have developed formal, written procedures. UW System institutions have also used some methods that are commonly accepted to remove data from the hard drives of surplus computers.

However, the current procedures and practices leave open the possibility of some surplus computers being disposed of without having the data securely removed from the hard drives prior to disposal. Thus, we have recommended that:

- UW System institutions develop formal policies and procedures for disposing of surplus computers, incorporating secure data removal methods in their policies and procedures;
- UW System institutions consider purchasing “Keep-Your-Hard-Drive” services if such services are available; and
- UW System Administration and UW System institutions include a provision in personal computer contracts to shield the UW System from potential liability resulting from inappropriate disclosure of confidential information through the computer vendors’ or manufacturers’ failure to securely remove data from hard drives that UW System institutions return for replacement.

Appendix 1

UW-EXTENSION INFORMATION TECHNOLOGY EQUIPMENT DISPOSAL POLICY

The purpose of this policy is to ensure appropriate destruction of proprietary, sensitive, or personal information when UW-Extension disposes of, or sends to surplus, information technology equipment.

When information technology equipment is sent to surplus or is disposed of, all data must be removed from the media in such a way that it is beyond the reach of all ordinary and most laboratory recovery methods. Simply erasing the data or reformatting the media is not acceptable because it does not prevent data from being recovered by technical means. Information technology departments throughout UW-Extension can assist users in data sanitization.

Three methods are acceptable for secure data sanitization:

1. Degaussing

Degaussing magnetically erases data from magnetic media and hard drives. Before attempting any degaussing process, please consult an information technology professional. Degaussing may damage information technology electronics, making them unusable.

2. Overwriting

The disk may be completely overwritten with data so that the old data cannot be recovered. The number of times data must be overwritten depends upon the sensitivity of the data. The U.S. Department of Defense has defined a clearing and sanitizing standard (DoD 5220.22-M) that is used to meet their requirements. There are a number of free and commercial products that can be used to sanitize the disks, including those that meet DoD standards.

3. Physical Destruction

As a last resort, information technology equipment can be "totally destroyed". For UW-Extension information technology equipment, the degaussing or overwriting processes are likely sufficient, but when the level of data sensitivity calls for it, total destruction of the equipment can be undertaken if there is no longer any use for the equipment or if the equipment no longer has any value. The National Industrial Security Program Operating Manual used by national security agencies defines "destroy" as "to disintegrate, incinerate, pulverize, shred or melt the equipment."

Appendix 2

UNIVERSITY OF WASHINGTON **NOTICE OF COMPUTER EQUIPMENT ELECTRONIC STORAGE DEVICE CLEANING PROPERTY AND TRANSPORT SERVICES, SURPLUS PROPERTY**

To ensure compliance with federal and state statutes associated with confidential information, such as the Health Information Portability and Accountability Act of 1996 (HIPAA) and the Family Educational Rights and Privacy Act (FERPA), the University of Washington requires the destruction of all data in computers or electronic storage devices* prior to surplusing. All software and data files **MUST** be electronically purged according to the methods approved by Computing and Communications (see reverse).

Computer* hardware sent to Surplus Property is sold to non-profit organizations and the general public. Any software and data files left on a hard drive, main frame, server, and/or electronic storage device could potentially be retrieved. This oversight can lead to conflicts with software license agreements and/or result in unauthorized access to University documents.

Files that are not past their retention period (see www.washington.edu/admin/recmgt) must be migrated to current systems or another suitable storage format.

After all software and data files have been **PURGED, COMPLETE, SIGN, and AFFIX** the form to the unit being surplused.

If the computer* is **not** working, UW Departments can elect to have Surplus Property purge the computer* and charge the departments' budget \$25.00 per computer*. If the computer* is **not** working, check the appropriate box on the form which indicates you have elected to have Surplus Property purge the computer*; please **COMPLETE, SIGN, and AFFIX** the form to the unit.

NOTE: One form must be completed for EACH computer*

Surplus Property staff must audit all working computers to verify if software and data files have been removed. **If any computer* surplused is found to contain data, the surplusing department will be charged for the audit and special handling costs which equal \$100.00 per unit**.** In addition, if any computer surplused is found to contain patient health information as defined by UWMC Patient Data Services, the name of the signer on the form will be forwarded to the appropriate Human Resources office as required under HIPAA.

***Computer or electronic storage device including but not limited to hard drive, laptop, server, main frame, or handheld computer, e.g. Palm or Visor**

****If additional labor time and/or expertise from C&C is required to properly prepare equipment for sale or disposal, additional costs will be charged to the surplusing department above the base fee of \$100.00.**

RESOURCES

Departments without local computing support needing to purge information on computer equipment may contact C&C's Computer Maintenance Group (CMG).

CMG offers fee-based assistance and may be reached at:

Phone#: 206/543-7865

Email: cmg@cac.washington.edu

UWMC/HMC staff: for more information on electronically purging computer equipment contact Medical Center Information Services (MCIS) at mcsos@u.washington.edu

METHODS FOR DESTROYING DATA FROM COMPUTER EQUIPMENT

Prior to surplusing, computers* must have all software and data files destroyed. Any electronic destruction method must include at least a three pass binary overwrite method.

I have electronically purged software and data files from this computer*, detailed below, by utilizing one of the following approved methods:

- eAutoclave (<http://www.washington.edu/computing/software/otherresources/autoclave/>)
- Norton utilities (<http://www.symantec.com>)
- PGP (<http://web.mit.edu/network/pgp.html>)
- Burn for Mac (<http://www.thenextwave.com/burnHP.html>)
- TechTool Pro for Mac (<http://www.micromat.com>)
- I have not used one of the approved methods listed above, but did use the following method that includes at least a three-pass binary overwrite (specify in detail):

- The equipment listed below is not in working condition and I request Surplus Property to purge the computer* and charge my budget \$25.00 per computer*. **NOTE: Destroying the hard drive is no longer an approved option, effective February 2003. (RCW prohibits the destruction of state property.)**

SIGNATURE

Name (please print): _____

Signature: _____ Date: _____

Department: _____ Phone: _____

COMPUTING & COMMUNICATIONS SECTION

This section is to be completed by C&C if the department was involved in the data destruction process. C&C provided the following support services and made the following determination:

Name (please print): _____

C&C Signature: _____ Date: _____

EQUIPMENT

Description of Computer*: _____

UW Inventory Number: _____ Serial Number: _____

***Computer or electronic storage device including but not limited to hard drive, laptop, server, main frame, or handheld computer, e.g. Palm or Visor**

If you have any questions, please contact Surplus Property at 206/685-1573 or via email at: surplus2@u.washington.edu