

**Office of Operations Review and Audit**



**Program Review**

**Protecting Computer Networks  
and Data in the UW System**

**March 2008**

## Table of Contents

	<b>Page</b>
Executive Summary	i
Scope	1
Background	1
Discussion and Recommendations	2
Information Protection Laws and Disclosures	3
IT Organization and Staffing	5
IT Structures	5
Computer Security Function Staffing	6
Computer Security Policies and Procedures	10
Principal UW Computer Security Policy	10
Issue-Specific Institutional Policies	11
Computer Security Incident Response	12
Network and Data Access	13
Security Hardware and Software	13
Passwords	17
Physical Access to Data Centers and Network Equipment	17
IT User Education	18
Conclusion	20
Appendix	22

## **EXECUTIVE SUMMARY**

Institutions of higher education rely on information technology (IT) for many of their critical operations, including admissions, financial aid, student records, research, and instruction. Increased use of IT increases the risk of unauthorized disclosure of confidential data. College and university IT leaders identify computer security as one of the top ten IT issues their institutions face. The Office of Operations Review and Audit reviewed efforts to protect computer networks and private electronic data in the UW System. The review examined: information protection laws, computer security staffing, policies and procedures related to computer security, access to computer networks and data, and user education. The review also examined computer security staffing, policies, and practices at other higher education institutions. This review is not a security audit which, by definition, includes systematic and technical assessments of IT systems, applications, processes, and specific measures.

### **Information Protection Laws and Disclosures**

Protection of personally identifiable information is governed by a combination of federal and state laws, UW policies, and consumer credit card policies. These include the Family Educational Rights and Privacy Act (FERPA); the Health Insurance Portability and Accountability Act (HIPAA); the Gramm-Leach Bliley Act (GLBA); UW Regent Policy Document (RPD) 25-3 covering the use of IT resources; the Payment Card Industry (PCI) Data Security Standards; and s. 895.507, Wis. Stats.

According to the Privacy Rights Clearinghouse, a total of 190 data breaches or unauthorized disclosures involving colleges and universities in the United States were reported between January 1, 2005 and December 31, 2007. More than four million students, faculty, staff, and alumni records were involved in these 190 breaches. These breaches resulted from hackers, stolen computers or storage media, and accidental or unintentional acts by internal staff.

### **IT Organization and Staffing**

UW institutions have developed their computer security function in one of two ways: by establishing an office or appointing a full-time information security officer, or by assigning computer security duties to certain IT staff as part of the staff's varied IT responsibilities. Having a person or an office solely responsible for computer security is recommended by various IT security professional organizations. Many institutions of higher education have also established a central security office or officer.

A security function enables an institution to be more proactive in addressing computer security issues and coordinating computer security efforts across the institution. In order to ensure that appropriate attention is paid to computer security, the report recommends that UW institutions, if they have not already done so, designate a computer security officer position that has computer security as its primary responsibility and that requires the necessary computer security skills. Two UW institutions were recently able to establish such a position through internal reallocations.

## **Computer Security Policies and Procedures**

UW Regent Policy Document (RPD) 25-3, “Policy on Use of University Information Technology Resources,” was not intended to be a computer security policy. However, RPD 25-3 does require users to take reasonable care to ensure that unauthorized persons are not able to use their access to UW computer systems and encourages UW institutions to protect electronic documents containing private and confidential information. In addition to RPD 25-3, UW institutions have adopted institution-level policies to address a wide range of areas and issues. Some universities in other states have developed a comprehensive information security policy that typically goes beyond acceptable use of IT resources. A common theme in many of these policies is defining and classifying data that need protection. Only two UW institutions address data classifications in their policies. The report recommends that UW System institutions, if they have not done so, develop an institutional policy that identifies the specific types of data that need additional protection.

All UW institutions visited for this review reported having procedures for reporting a computer security incident – any real or suspected adverse event in relation to the security of a computer system or computer network. However, only two UW institutions have formal, written procedures documenting the process for responding to a computer security incident. To ensure that procedures are in place when data breaches are detected and when statutory notification requirements need to be considered, the report recommends that UW System institutions develop formal, written policies and procedures on computer security incident response.

## **Network and Data Access**

UW System institutions have implemented some security hardware and software common to the IT industry and institutions of higher education. These include firewalls, anti-virus software, and anti-spyware software. Most UW institutions require password standards and regular password changes in accessing the main campus networks. UW institutions have also implemented some common measures to protect their data centers. However, the nature of IT threats is continually changing. Therefore, the report recommends that all UW System institutions perform periodic vulnerability assessments of their networks, including reviewing security hardware and software, passwords, and access to data centers and departmental servers, and that they mitigate any identified risks accordingly.

## **IT User Education**

UW System institutions have offered varying degrees of computer security awareness education for their campus computer users. Education is provided through campus websites, flyers, posters, and mass e-mails. Information provided covers issues such as passwords, patches, data storage, anti-virus protection, and anti-spyware. The National Institute of Standards and Technology recommends specific information that should be provided in a computer security education program. Since it is critical that computer users are aware of threats and follow good computer security practices, the report recommends that UW System institutions assess their education programs for computer users to ensure the programs cover information that is essential for safe and secure IT usage.

## **SCOPE**

The University of Wisconsin (UW) System Office of Operations Review and Audit reviewed efforts to protect computer networks and private electronic data in the UW System. This review is not a computer security audit which, by definition, includes systematic and technical assessments of information technology (IT) systems, applications, or processes. While we examined security measures UW System institutions have implemented, we did not conduct a technical assessment of these measures to determine their effectiveness or adequacy. The review focused on IT staffing, policies and procedures, access, and user education.

To conduct this review, we: 1) analyzed UW System and institutional policies related to computer security; 2) researched computer security staffing, policies, and practices at other higher education institutions; and 3) visited UW-Madison, Milwaukee, Oshkosh, Parkside, River Falls, Whitewater, UW Colleges, and UW-Extension and conducted surveys and telephone interviews with staff at all UW campuses we did not visit. UW staff we interviewed included chief information officers (CIOs), information security officers, network administrators, and data center managers. During the visits, we also walked through some data centers to examine physical security measures at these centers.

## **BACKGROUND**

Information technology permeates every aspect of higher education operations. Institutions of higher education rely on IT for more and more of their critical operations, including admissions, financial aid, accounts payable, accounts receivable, student records, research, and instruction. IT appears to have increased productivity and efficiency and reduced costs in some of these operations.<sup>1, 2, 3</sup> IT also increases access to higher education and often improves the quality of the student learning experience. At the same time, however, increased use of IT increases certain associated risks. According to the 2007 Current Issues Survey by EDUCAUSE, an organization that promotes intelligent use of IT in higher education, U.S. college and university IT leaders identified computer security as one of the top ten IT issues facing their institutions.<sup>4</sup>

One concern about computer security stems from the potential effects of unauthorized disclosures of personally identifiable information or breaches. Data breaches can and have resulted in:

- ***Identity theft***: Identity theft involves the use of another individual's personally identifiable information to commit fraud. A survey conducted by the Federal Trade Commission (FTC)

<sup>1</sup> Twigg, Carol. "Improving Quality and Reducing Costs: Designs for Effective Learning." *Change*, July/August 2003.

<sup>2</sup> Frazier, Lavon R. "An Admissions Process Transformed with Technology." *EDUCAUSE Quarterly*, November 2000.

<sup>3</sup> Newpher, Cameron. "An IT Evolution in the Classroom." *Techniques: Connecting Education and Career*, May 2006.

<sup>4</sup> Camp, John S., Peter B. DeBlois, and the EDUCAUSE Current Issues Committee. "Current Issues Survey Report, 2007." *EDUCAUSE Quarterly*, Number 2, 2007.

estimated that 3.6 million households, or 3.1 percent of the households in the United States, became victims of identity theft in 2004.<sup>5</sup>

- ***Financial losses:*** When a breach is detected, resources are needed to address the breach. Where data loss occurs, legal actions could be and have been brought against colleges and universities. While most of the financial losses resulting from identity theft are borne by financial institutions, some colleges and universities where data loss occurred have had to pay the costs for credit monitoring for individuals affected by the breach. Gartner, an IT research company, estimated that a mid-range breach of tens of thousands of records would cost an organization between \$90 and \$100 per affected record.<sup>6</sup> A study by Forrester Research found that the average security breach can cost a company between \$90 and \$305 per lost record.<sup>7</sup>
- ***Damaged reputation:*** Students, staff, faculty, and alumni trust colleges and universities with the safekeeping of their personal data. Data losses tarnish colleges' and universities' reputations if it is perceived that colleges and universities contributed to or were responsible for the losses.
- ***Violation of law, policies, and standards:*** Protecting private information of UW students, faculty, staff, and alumni is required by: 1) certain federal and state laws, such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA); 2) by UW policies, including a Board of Regents policy on use of university information technology resources; and 3) by data security standards, such as the Payment Card Industry (PCI) Data Security Standards. Unauthorized disclosure of private information may be deemed violations of these laws, policies, and standards.

The literature on computer security and the opinions of various IT security experts indicate that protecting personal data and computer networks will continue to be an issue and a challenge for colleges and universities. According to the Chronicle of Higher Education, "increased identity theft, online stalking, cyberterrorism," and "increased willful disruption of campus networks" are among the ten trends to watch in campus technology.<sup>8</sup>

## **DISCUSSION AND RECOMMENDATIONS**

There appears to be a growing concern about the unauthorized disclosure of private information, as evidenced by the federal and state legislation related to privacy. Protecting computer networks and data (also referred to as computer or information security in this report) is complex, however. Effective computer or information security requires the integration of

<sup>5</sup> Baum, Katrina. "Identify Theft, 2004." *Bureau of Justice Statistics Bulletin*, April 2006.

<sup>6</sup> Wood, Lamont. "The Cold, Hard Costs of Data Exposure," September 27, 2006, <<http://www.esj.com/news/print.asp?editorialsId=2169>>.

<sup>7</sup> Gaudin, Sharon. "Security Breach Cost \$90 to \$305 Per Lost Record." *InformationWeek*. April 11, 2007.

<sup>8</sup> Martin, James and James E. Samels. "10 Trends to Watch in Campus Technology – Plus 8 Myths and 7 Key Skills for CIO's." *The Chronicle of Higher Education*, January 7, 2007, <<http://chronicle.com/weekly/v52/i18/18b00701.htm>>.

technologies, policies, and people. This report discusses: 1) information protection laws and disclosures; 2) IT organization and staffing; 3) IT policies and procedures; 4) network and data access; and 5) IT user education.

## **INFORMATION PROTECTION LAWS AND DISCLOSURES**

Protection of personally identifiable information is governed by a combination of federal and state laws, UW policies, and consumer credit card policies:

- *The Family Educational Rights and Privacy Act (FERPA)*: FERPA is a federal law that protects the privacy of education records. Schools may disclose, without consent, directory information, such as student name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. Schools may disclose, without consent, personally identifiable information from education records only to certain parties and under certain circumstances, such as to school officials with a legitimate interest, to appropriate parties in connection with financial aid to the student, and to appropriate officials in cases of health and safety emergencies.
- *The Health Insurance Portability and Accountability Act (HIPAA)*: HIPAA protects individually identifiable health information in certain circumstances. Individually identifiable health information includes common identifiers, such as name, address, date of birth, and Social Security number.
- *The Gramm-Leach Bliley Act (GLBA)*: GLBA protects personally identifiable financial information. GLBA also requires covered entities to implement a comprehensive information security program along with a risk assessment process.
- *Regents Policy Document (RPD) 25-3*: RPD 25-3, “Policy on Use of University Information Technology Resources,” requires UW institutions to take reasonable precautions to protect electronic documents containing private and confidential information.
- *Payment Card Industry (PCI) Data Security Standards*: The major credit card associations -- Visa, MasterCard, American Express, and Discover -- require that credit card processors and merchants accepting payment cards and storing, processing, or transmitting credit cardholder data implement certain security measures and computer system configurations.
- *Section 895.507, Wis. Stats.*: Wisconsin is one of 39 states that have enacted a data security breach law. Section 895.507, Wis. Stats. requires businesses and organizations operating in Wisconsin, including the UW System, to notify individuals to whom the personal information pertains when their information has been disclosed to an unauthorized person. Under s. 895.507, Wis. Stats., which went into effect on March 31, 2006, a notification is only required if the disclosure creates a material risk of identity theft or fraud to the individuals to whom the personal information pertains.

The Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization, began to track incidents of data loss and theft in 2005. The Clearinghouse does not define data-loss incidents but, rather, compiles data that entities are required to report under their own states' security breach notification laws. States' reporting requirements vary; thus, the reported incidents may or may not have involved information that was ultimately used for identify theft, monetary theft, or similar purposes. Between January 1, 2005 and December 31, 2007, a total of 190 data breaches or unauthorized disclosures at colleges and universities in the United States were reported. Over 4.7 million students, faculty, staff, and alumni records were involved in these 190 breaches or disclosures. Table 1 shows the number of data breaches or disclosures, records involved, and institutions with the largest number of records involved.

**Table 1: Examples of Data Breaches at Institutions of Higher Education\*  
(Calendar Years 2005, 2006, and 2007)**

<b>Year</b>	<b>Number of Breaches</b>	<b>Total Records Involved</b>	<b>Institutions with Largest Number of Records Involved</b>
2005	57	1.7 million	University of Southern California (admissions); University of Hawaii (various); Boston College (alumni); Tufts University (alumni); University of Utah (personnel); and University of California Berkeley (research).
2006	65	2.1 million	University of California Los Angeles (financial aid); Western Illinois University (admissions, bookstore, financial aid, and hotel); University of Texas (various); Ohio University (health); Sacred Heart University (recruitment); and Metropolitan State College (enrollment).
2007	68	830,500	Community College of Southern Nevada (various); Stonybrook University (various); University of Louisiana System (testing and personnel); University of Idaho (various); and East Carolina University (various).

Source: Analysis is based on data obtained from the Attrition Dataloss Listserve. The Privacy Rights Clearinghouse also obtains its data from this listserve.

\* Excludes university hospitals and medical facilities.

These data breaches reported by the Privacy Rights Clearinghouse represent only a subset of breaches that occurred. The breaches reported were primarily from states that have laws in effect requiring notification of individuals affected by the breach. As noted, only 39 of the 50 states, including Wisconsin, have passed such laws.

Outside hackers were involved in 60 percent of the reported incidents in 2005. In 2007, only 25 percent of the reported incidents were the result of hackers. Since 2005, stolen laptops and storage devices accounted for an increasing number of the reported incidents. Other incidents were the result of accidental or unintentional acts by internal staff, such as posting files that contain private information on the internet, sending e-mails that contain private information to unauthorized individuals, and losing storage media that contain private data.

## **IT ORGANIZATION AND STAFFING**

A successful computer security program involves identifying the risks, developing measures and controls to mitigate those risks, monitoring the known risks, ensuring compliance with policies and procedures, and responding to incidents promptly and appropriately when they occur. We reviewed UW institutions' IT organizational structures and examined staffing levels assigned to perform these tasks.

### **IT Structures**

How the IT function is structured influences strategies to protect computer networks and confidential data that are stored on these networks. IT organizational structures vary across UW System institutions. For example:

- Most UW institutions, including UW-Madison, Milwaukee, and Oshkosh, have decentralized IT operations, through which various major departments have their own IT staff and even operate their own computer networks.
- UW-Green Bay is the only UW institution where a central IT department provides all of the IT support and manages all of the computer networks.
- UW-Platteville and UW Colleges/Extension have variations of a centralized IT structure. UW-Platteville IT hosts and maintains all campus networks, and IT support staff are part of a central IT unit, but the staff members are physically located at the respective campus departments. UW Colleges/Extension's central IT unit manages the networks connecting all two-year campuses, but individual campuses operate and maintain their own campus networks.

Despite the variations, all UW System institutions have individuals who are responsible for computer security. These include chief information officers (CIOs), IT committees, and IT security officers or staff:

- The CIOs have overall responsibility for IT security at their institutions. At most UW institutions, the CIOs report to the Provosts. However, the CIOs at UW-Stout and UW Colleges/Extension report to the Chancellor. The CIO at UW-River Falls reports to the Vice Chancellor for Administration and Finance.
- Seven of the eight UW institutions we visited have at least one IT committee. These committees typically review and make recommendations on campus IT strategic plans, issues, and policies. Some IT committees are part of shared governance, which means that faculty, staff, and students participate. Others are standing subcommittees of the faculty committee or advisory committees to the CIOs. New institutional IT policies are typically brought to these committees, although committee approval is not required.
- Each UW institution has assigned day-to-day computer security responsibilities to certain staff. At UW-Madison, Milwaukee, and Whitewater, these staff members hold the title of

information or computer security officer, and computer security is their primary responsibility. At other UW institutions, the network administrators or data center managers have security duties as one part of their other responsibilities. IT security duties include coordinating the deployment of security measures and policies, monitoring computer security threats, investigating and responding to computer security incidents, and coordinating computer security awareness education for campus IT users.

### **Computer Security Function Staffing**

Literature we reviewed indicates there is a long-established practice in the IT industry of having a central person or unit responsible solely for computer security. This might be an information security officer (ISO), computer security officer (CSO), or an information security office. Various standards bodies and organizations also recommend staff be assigned specifically to computer security, because computer security requires specialized skills and competencies and involves coordination of computer security efforts across an organization. For example, information security standards issued by the International Organization for Standardization, an international standards-setting body, specify that computer security responsibilities should be assigned to a single manager within the organization. The Federal Information Security Management Act (FISMA) of 2002 requires federal agencies to designate a senior agency information security officer. The officer must possess information security qualifications and have information security duties as his/her primary duty. In addition, EDUCAUSE's assessment tool for higher education delineates these principles pertaining to the computer security function:

- the person assigned to the computer security function should have computer security as his/her primary responsibility;
- leaders and staff of the computer security function should have the necessary experience, qualifications, and skills; and
- the computer security function should have the resources and authority it needs to manage and ensure compliance with the computer security program across the organization.

UW institutions have developed their computer security functions in one of two ways. UW-Madison, Milwaukee, and Whitewater established an office or appointed full-time information security officers devoted exclusively to computer security. At the remaining UW institutions, certain IT staff members are assigned computer security as part of their varied IT responsibilities. Some UW institutions, such as UW-Green Bay, La Crosse, Oshkosh, Stevens Point, Superior, and UW Colleges/Extension, assign a specific percentage of the staff members' position descriptions to computer security. However, computer security is not their primary responsibility. Table 2 on the next page shows the staffing levels assigned to the computer security function.

At the time of our visits, three UW institutions we visited were in the process of reorganizing or were planning to restructure their IT operations. Changes being considered included centralizing the IT organization, consolidating or reorganizing the network infrastructure, and refining IT

**Table 2: Computer Security Staffing and Staff Reporting  
(as of February 2008)**

<b>UW Institution</b>	<b>Security Staffing</b>	<b>Reporting Structure</b>
Eau Claire	At least three staff members in Technical Services handle security as part of their responsibilities. No specific percentage of job time is assigned.	Manager of Technical Services reports to the director of Learning and Technology Services. The Director of Learning and Technology Services reports to the Provost. The CIO reports to both the Director of Learning Technology Services and the Provost.
Green Bay	Ten percent of Network Manager's position description is assigned to security. UW-Green Bay plans to eventually assign one full-time equivalent staff to computer security.	Network Manager reports to the CIO.
La Crosse	An Information System supervisor in Network Services is the designated chief information security officer, and 15 percent of the position is assigned to security. Individuals from UW-La Crosse's Server Group, Enterprise Systems, and Help Desk Support also assist in addressing security issues.	The Information System supervisor reports to the CIO.
Madison	Within the Office of Campus Information Security, 12 full-time positions are assigned to computer security exclusively.	Director of the Information Security Office reports to the CIO.
Milwaukee	Three full-time staff within the Information Security Office are assigned to computer security exclusively.	Information Security Office Director reports to the CIO.
Oshkosh	The Database Administrator holds the title of Data Security Officer, and 20 percent of his time is assigned to data security. The Network Administrator also handles security as part of her responsibilities, but no specific percentage of job time is assigned.	The Database Administrator/Data Security Officer and the Network Administrator report to the CIO.
Parkside	The Network Services Director handles security as part of his responsibilities. No specific percentage of job time is assigned. A requested desktop architect position will also have computer security responsibilities.	Network Services Director reports to the CIO.
Platteville	Security responsibilities are included in the two network services staff's position description. No specific percentage of job time is assigned.	Network services staff report to the CIO.

<b>UW Institution</b>	<b>Security Staffing</b>	<b>Reporting Structure</b>
River Falls	Network Services Manager handles security as part of her responsibilities. No specific percentage of job time is assigned.	Network Services Manager reports to the CIO.
Stevens Point	One half-time security officer position and two other staff serve as the security team.	Security Officer reports to the CIO.
Stout	Multiple Network Service and Support staff handle security as part of their responsibilities. No specific percentage of job time is assigned.	The Network Service and Support Supervisor reports to the CIO.
Superior	Twenty percent of Network Supervisor's position description is assigned to network security.	Network Supervisor reports to the CIO.
Whitewater	One full-time Information Security Officer position is assigned to computer security exclusively.	Information Security Officer reports to the CIO.
Colleges/ Extension	Forty percent of the Network Administrator's position and 40 percent of the Network/Data Center Manager's position are assigned to security responsibilities.	The Network Administrator reports to the Network/Data Center Manager, who then reports to the CIO on security matters.

Source: UW Institutions.

staff roles and responsibilities. Therefore, staffing levels and responsibilities are likely to change when the reorganizations are completed.

It appears that the practice of having a dedicated computer or information security office or officer has gained popularity among colleges and universities. For example, we obtained the results of a 2005 EDUCAUSE survey and a survey conducted in 2006 by the security officer at the University of South Carolina on the number of staff positions dedicated to computer security at colleges and universities. Although direct comparisons with the UW System are not valid because of variations in institutions' staff size, enrollment, IT operations, and resources, the two surveys made some noteworthy findings:

- approximately 91 percent of the 46 institutions that responded to the University of South Carolina survey and 61 percent of those institutions responding to EDUCAUSE's 2005 survey had at least one full-time staff position devoted to computer security exclusively;
- thirty-five percent of the institutions in EDUCAUSE's 2005 survey had an IT security officer or equivalent, an increase from 22 percent in 2003;
- sixty-two percent of the institutions in EDUCAUSE's 2005 survey had one central IT security office, an increase from 39 percent in 2003; and
- day-to-day responsibilities for computer security have shifted away from directors of network services to computer security officers (CSOs).

The size of the computer security function depends on the institutions' vulnerabilities, which may vary from institution to institution. UW institutions are in the best position to determine their unique vulnerabilities and what risks they can tolerate. To make this determination, and because the vulnerabilities may change, UW institutions need an effective computer security function. Having an effective security function does not eliminate the risks, but the function enables institutions to be more proactive in addressing computer security by: 1) assessing computer security weaknesses, 2) developing policies, standards, and procedures to alleviate the identified weaknesses, and 3) developing programs to educate university computer users about safe and secure computing. An effective security function would also enable institutions to coordinate computer security efforts across the campus.

Staff with computer security skills and competencies are necessary for an effective computer security function. Computer security skills and competencies can be built through training, and a number of different training-based certificates are available. At the time of the review, there were certified computer security staff at UW-Madison, Milwaukee, Stevens Point, Whitewater, and UW Colleges/Extension. In order to ensure that appropriate attention is paid to computer security, ***we recommend that UW institutions, if they have not done so, designate a computer security officer position that has computer security as its primary responsibility and that requires the necessary computer security skills and competencies.***

Some smaller UW System institutions indicated that resource constraints would present difficulties in designating a computer security officer position with computer security as its primary responsibility. However, UW-Green Bay is in the process of reallocating staff resources to increase the amount of time devoted to computer security. UW-Green Bay plans to increase the amount of time currently devoted to security from 10 percent to 60 or 65 percent in the near future, and to eventually assign one full-time equivalent staff to computer security.

Seeking additional funding specifically for computer security is an option, but a more realistic alternative may be to find potential cost savings from existing IT operations. The CIOs at UW-Milwaukee and Whitewater reported that their security functions were created through internal reallocation and reorganization and not through positions being added. For example, UW-Milwaukee's IT Division consolidated its IT operations in 2006, reducing seven departments to four, and used the savings from administrative positions to create its information security office. UW System Administration made computer security the primary responsibility of the IT security officer position through internal reallocation in 2003.

Identifying specific ways to maximize the use of IT resources is beyond the scope of this review. However, during our research we did find examples where some colleges and universities have achieved costs savings:

- The University of Houston reported saving about \$1 million annually by developing web-based questions and answers to address the previous phone and e-mail workloads across the major functional areas, such as admissions, financial aid, and the registrar's office.
- The University of North Carolina at Charlotte determined that one-third of its 4,500 personal computers can be replaced with network computers without hard drives, CD-ROM players,

and expansion slots (known as thin clients) without sacrificing functionality. The university estimated that it would save about \$400,000 to \$600,000 a year on acquisition costs.

- In 2003, Brevard Community College (Florida) replaced its communication system with Voice over Internet Protocol (VoIP), a technology that allows voice conversations to be routed through the Internet. At the time, the college was using an analog switch and it was showing signs of failure. Brevard Community College estimated that the switch to VoIP resulted in one-time savings of about \$600,000, compared to the costs of replacing the existing lines at its campuses.

## **COMPUTER SECURITY POLICIES AND PROCEDURES**

According to IT security literature, sound policy is the cornerstone of effective strategy to protect computer networks and data.<sup>9</sup> Policies are intended to establish the standards or lay out the expectations to be followed. We discussed with UW institution staff the extent to which existing Board of Regents or systemwide IT policies provide UW institutions with clear expectations about computer security and adequate authority to enforce compliance with their computer security measures. We also obtained from UW institution staff and IT websites formal computer security-related policies to determine what computer security areas or issues are addressed by the institutions.

### **Principal UW Computer Security Policy**

Literature indicates universities have generally addressed computer security issues through their acceptable use policies,<sup>10</sup> which set forth the principles that govern appropriate use of university computers and networks. This is also true in the UW System.

RPD 25-3, “Policy on Use of University Information Technology Resources,” was not intended to be a computer security policy. However, RPD 25-3 does require users of UW IT resources to “take reasonable care to ensure that unauthorized persons are not able to use their access to the system.” RPD 25-3 also encourages UW institutions to “take reasonable precautions to protect electronic documents containing private and confidential information.” (RPD 25-3 is included as Appendix 1.)

In addition, most UW institutions have adopted their own institutional policies on acceptable use, which are an adaptation or expansion of RPD 25-3. Most UW staff we interviewed also reported that RPD 25-3 provides adequate authority for IT staff to confront any situations where computer security might be compromised.

<sup>9</sup> Boes, Richard, Tom Cramer, Vicky Dean, Roger Hanson, and Nan McKenna. “Campus IT Security: Governance, Strategy, Policy, and Enforcement.” *EDUCAUSE Center for Applied Research*, Research Bulletin, Volume 2006, Issue 17, August 15, 2006.

<sup>10</sup> Luker, Mark and Rodney Petersen (Editors). *Computer and Network Security in Higher Education*, (Jossey-Bass: 2003)

### Issue-Specific Institutional Policies

Even though some UW System institutions do not have formal policies on a specific area or issue, they have adopted guidelines or practices that offer some security protection. As shown in Table 3, UW institutions have adopted institution-level policies to address a wide range of IT areas or issues.

**Table 3: Areas or Issues Addressed by Institutional Policies**

Area or Issue	Policy Purposes	UW Institutions with Policies in Place
Acceptable/ appropriate use	Establishes expectations for the use of university IT resources.	Green Bay, Madison, Milwaukee, La Crosse, Oshkosh, Platteville, River Falls, Stevens Point, Superior, Whitewater, and Colleges/Extension.
Network password	Establishes the standards for password strength and complexity.	Green Bay, Eau Claire, Madison, Stevens Point, Superior, and Whitewater.
Network access and use	Recommends or ensures that all devices connected and with access to the networks are administered in a way that minimizes problems for users of the network and maintains the security of data stored on the networks.	Green Bay, Eau Claire, Madison, Milwaukee, Parkside, River Falls, Whitewater, and Colleges/Extension.
Information or data access and security	Establishes the framework for computer security on campus.	Green Bay, La Crosse, Madison, Milwaukee, Oshkosh, Parkside, Platteville, River Falls, Superior, and Whitewater.
E-mail	Establishes appropriate use of e-mail resources.	Green Bay, Madison, Oshkosh, Parkside, River Falls, Stevens Point, and Whitewater. Superior was drafting a policy.
Electronic devices	Establishes standards for devices connected to university networks.	Madison, Oshkosh, Platteville, Stevens Point, Superior, and Whitewater.
Remote access and wireless	Establishes guidelines and procedures for remote access and wireless.	Green Bay, La Crosse, Madison, Oshkosh, and River Falls.
Software and/or hardware	Establishes standards for hardware and appropriate use of software.	Green Bay, Milwaukee, Oshkosh, Platteville, River Falls, Stevens Point, Whitewater, and Colleges/Extension.

Source: UW institutions and UW institution websites.

We researched policies related to computer security at the University of Arizona, University of California, California State University, University of Colorado, University of Georgia, Indiana University, University of Illinois, University of Iowa, Ohio State University, University of Michigan, University of Minnesota, Minnesota State Colleges and Universities, University of Missouri, and University of Texas. As in the UW System, individual institutions within these university systems have adopted institution policies addressing a wide range of computer security issues.

While this range of security issues is important and should be addressed as time and resources allow, we found that institutions of higher education in other states are devoting resources to develop a comprehensive information security policy. This policy goes beyond acceptable use. These policies define data that need protection and specify the roles and responsibilities of users, data custodians, departments, and central IT security staff.

A number of UW institutions have some type of information security policy. However, only UW-Madison's and UW-Milwaukee's information security policies actually designate certain personal data for enhanced protection. At UW-Madison, information such as Social Security numbers, driver's license numbers, financial account numbers, DNA profile, biometric data, and protected health information, are designated restricted. University departments that process or store any of the restricted information are required to implement security measures consistent with the Payment Card Industry Data Security Standards. At UW-Milwaukee, data are classified as either confidential, sensitive, or public. UW-Milwaukee's guidelines provide recommendations as to the appropriate security measures for each class of data. Defining data that need priority for protection and what level of protection is acceptable is basic to computer security; however, few UW institutions address this area in their policies. ***We recommend that all UW System institutions, if they have not done so, develop an institutional policy that identifies the specific types of data that need additional protection.***

### **Computer Security Incident Response**

A criticism of some other universities that experienced data breaches was the slow response to security incidents or breaches and the delay in notifying individuals affected by the breaches. A security incident is defined as any real or suspected adverse event in relation to the security of computer systems or computer networks. Timely action to resolve the incident and to notify individuals affected is critical to mitigate the negative consequences of data breaches when they occur.

All UW institutions we visited reported having procedures for reporting security incidents. UW-Madison and UW-Milwaukee established on-line processes for reporting such incidents. At other UW institutions, institutional web sites, brochures, and e-mails to campus departments instruct campus computer users to contact the security officer, the network administrator, or the help desk when an incident is detected.

At UW institutions, upon receiving a report of an incident, the security officer or the network administrator is to assemble a team of appropriate staff to investigate and take the necessary actions to mitigate the incident. At UW-Milwaukee, the Campus Security Incident Response Team (CSIRT) includes staff from central IT services, department IT representatives, risk management, legal affairs, and internal audit. If the incident involves personal data, campus administration then makes the determination as to whether a notification is required.

At the time of our visits, only UW-Madison and Milwaukee have documented in writing the process of responding to computer security incidents. UW-Madison's policy and procedures on data security breach was still a draft. UW-Milwaukee had adopted a set of guidelines related to

incident response. These guidelines establish the expectations for central IT staff and define the roles of various offices.

The entire campus needs to know what to do and what steps to take when a data breach is detected. Having institutional policies and procedures on computer security incident response would establish roles, responsibilities, and the process for actions. It would also ensure that there is a process for implementing the notification requirements in s. 895.507, Wis. Stats., and would identify the staff who should be involved in the process. ***We recommend that UW System institutions that have not done so develop formal, written institutional policies and procedures on computer security incident response.*** At a minimum, the computer security incident response policy and procedures should:

- define computer security incidents that must be reported;
- establish a classification of incidents as a form of triage for proper response;
- establish the contact for incident reporting;
- establish the incident response team and its roles and responsibilities;
- specify documentation of the incident that must be maintained;
- establish a process for communicating the incident internally and externally; and
- establish a process for reviewing the resolution of the incident.

All eight UW System institutions we visited for this review reported at least one computer security incident within the last two years, but most of the known incidents did not involve personal data. For the few incidents that occurred after s. 895.507, Wis. Stats., went into effect and in which personal data were involved, UW institution staff indicated that they have complied with the requirements specified in the law. According to staff and documentation we reviewed, actions were taken on each incident that involved personal data. Actions included removing the information from the affected computer or server, changing passwords, patching the servers, reformatting the hard drives, disconnecting the server from the network, and placing the server behind a firewall.

## **NETWORK AND DATA ACCESS**

Controlling access to computer networks and data is a balancing act. Too many restrictions would render the network inefficient. At the same time, too few restrictions might allow unauthorized users easy access to the networks and private data stored on these networks. We examined security hardware and software UW institutions use to limit access to computer networks and data, password practices, and access to data centers and network equipment.

### **Security Hardware and Software**

Security hardware and software represent one layer of protection. There is not a single standard set of hardware and software that meets the needs of all UW institutions. What security hardware and software to use is best determined based on UW network configuration and resources.

UW System institutions establish and maintain integrated networks of computers. The typical UW computer network consists of multiple workstations or personal computers connected to a server, a computer dedicated to running certain applications or storing data via a hub or a switch.

With the exception of UW-Green Bay and UW-Platteville, IT operations are decentralized. Departments operate their own IT networks and often have hundreds of servers and workstations. For example, the Computer Science Department at UW-Madison maintains more than 100 servers and more than 600 workstations; UW-Milwaukee’s College of Letters and Science has 10 servers and more than 1,200 workstations. In addition to the workstations, UW institutions have both university-owned and personally-owned devices, such as routers, laptops, and hand-held devices, that are connected to the networks. UW System institutions also run a variety of operating systems on their networks, including Apple, Windows, Linux, and Novell. Windows is by far the most popular operating system run by UW System institutions, although some departments run Apple or Linux almost exclusively.

Considering the different network configurations and operating systems, various security hardware and software are available. However, these hardware and software are most effective when they work in tandem with each other and are integrated with other security measures. We found that all UW System institutions have implemented or were considering implementing some type of security hardware and software. Table 4 lists the security hardware and software used to protect UW institutions’ main campus networks.

**Table 4: Security Hardware and Software Used to Protect  
UW Institutions’ Main Campus Networks  
(as of February 2008)**

<b>Hardware or Software</b>	<b>Description and Purpose</b>	<b>Number of UW Institutions *</b>
Anti-spyware software	Spyware refers to software that is installed on computers, often without consent, to collect and track personal information, to track computer system configuration, and to display pop-up advertisements. Anti-spyware software protects against the installation of spyware and removes spyware that has already been installed.	All.
Anti-virus software	Viruses are programs or pieces of code that, once loaded onto the computers or networks, can cause computer or network disruption. Anti-virus software monitors the computer for virus activities and attempts to remove the detected viruses.	All.
Encryption **	Encryption is either a software or technology that transforms information into a form that is unintelligible except to those having the means for a reversible translation. Encryption is used in data storage as well as in data transmission.	All used encryption for web transactions. Eight institutions used encryption on their wireless networks. One institution was considering encryption for some laptops.

Hardware or Software	Description and Purpose	Number of UW Institutions *
Firewalls	Firewalls are hardware and software that enforce a boundary between networks. Perimeter firewalls control traffic between internal networks and external networks. Interior firewalls control traffic between segments of internal networks. Application firewalls limit access by the particular application to the operating system of a computer.	All.
Intrusion Detection System	Intrusion Detection System (IDS) is an application that monitors and analyzes network traffic, especially patterns of traffic that might indicate an attack.	Thirteen.
Intrusion Prevention System	Intrusion Prevention System (IPS) is a hardware or software device that monitors the network and blocks traffic from a suspect port.	Six.
Virtual Private Network (for remote access)	Virtual Private Network (VPN) is a secure tunnel used to connect remote sites or users together through the Internet.	Thirteen.

Source: UW staff interviews.

\* UW Colleges and UW-Extension are counted as two institutions.

\*\* Even though some UW System institutions do not use wireless encryption, sign-on is still required.

We researched the literature to determine how common the security hardware and software used by UW institutions are among businesses, governmental agencies, and institutions of higher education. We located two surveys. Both were conducted in 2005, and their results were released in 2006. One survey was conducted by the Computer Security Institute, a membership organization that serves IT security professionals, and the San Francisco Federal Bureau of Investigation’s Computer Intrusion Squad. In this CSI/FBI survey, 616 U.S. corporations, government agencies, financial institutions, medical institutions, and universities participated.<sup>11</sup> EDUCAUSE Center for Applied Research conducted the other survey, in which 492 colleges and universities in the U.S. and Canada participated.<sup>12</sup> Appendix 2 lists the results on the use of technologies. A direct comparison on the use of security hardware and software would be difficult as they may vary within each organization. Nonetheless, it appears that UW institutions have implemented some security hardware and software that are commonly used in the IT industry, including firewalls, anti-virus software, and anti-spyware software.

In addition to the various computer security hardware and software UW institutions have implemented, UW institutions we visited also have adopted a number of security practices as part of their overall strategies to restrict unauthorized access to computer networks and data. Examples include:

- *Establishing campus-wide security standards:* UW-Madison is rolling out the 21<sup>st</sup> Century Network project. The project will upgrade UW-Madison’s network. The project will also establish minimum security standards across the entire campus, including firewalls, an

<sup>11</sup> Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson. “2006 CSI/FBI Computer Crime and Security Survey.” Computer Security Institute.

<sup>12</sup> Kvaivik, Robert B., and John Voloudakis. “Safeguarding the Tower: IT Security in Higher Education 2006.” EDUCAUSE Center for Applied Research, Volume 6, 2006.

intrusion detection system (IDS), and anti-virus and anti-spyware programs. At the time of our visit, firewalls and IDS were only implemented at certain segments of the networks. When the project is completed, firewalls and IDS will be implemented at most, if not all, networks operating on campus.

- *Segmenting the networks*: Many schools and departments within a UW institution operate their own networks and have their own IT services. These networks are connected to the main campus network. To minimize disruption to the main campus networks should security breaches occur at the departmental networks, UW institutions segmented off these networks. All UW System institutions we visited reported the use of network segmentation, especially in the networks at student residence halls; however, the extent of use varied.
- *Conducting vulnerability assessments and security reviews*: A number of UW System institutions we visited have initiated security reviews of their computer networks or IT operations. UW-Milwaukee completed a review of its data center in 2006. UW-Parkside completed an evaluation of its IT operations in 2006, including a security review of its networks. UW-Madison and UW-Whitewater also regularly scan their network for vulnerabilities.
- *Consolidating and centralizing server maintenance*: Dedicated servers which run many of the main university applications and store university data must be properly maintained. In order to ensure that campus servers are properly maintained and secured, UW-Milwaukee and UW-Whitewater have collaborated with university departments to move their servers to campus data centers or to allow central IT staff to maintain these servers.

UW institutions we did not visit also indicated they have adopted some similar practices.

While controlling access to UW networks and data is done largely at the institution level, we identified noteworthy collaboration among UW System institutions on computer security. Since 2007, the UW chief information officers have been working with UW-Madison's Office of Campus Information Security to oversee the implementation of systemwide access to the PeopleSoft Shared Financial System (SFS). The implementation process entailed each UW System institution's conducting an internal assessment of its controls and procedures for authenticating users. The goals are to ensure a higher level of assurance for authenticating and authorizing users of SFS and other systems, and to secure the databases and directories where user access credentials are stored.

The collaboration also has extended to training and educational materials. Examples of collaboration include systemwide training hosted and provided by the UW-Madison Office of Campus Information Security and UW-Green Bay's adoption of educational materials from UW-Milwaukee.

## **Passwords**

Passwords are the most common mechanism to authenticate user access. Regular password changes and strong passwords, which typically include six characters or more and contain a mixture of upper case and lower case letters, digits, and special characters, are recommended best practices for computer security. Weak passwords make it easier for hackers to crack and assume the individual's identity to access the networks and data. We examined UW institution password requirements.

In 2006, UW System Administration (UWSA) adopted a password policy for UWSA computer users, requiring complex passwords. The UWSA password requirements were used as a template by UW System institutions. All but one UW institution requires complex passwords, and three UW institutions do not require regular password changes. The systemwide credential assessment process led by the UW-Madison Office of Campus Information Security for the PeopleSoft Shared Financial System will eventually lead to all UW System institutions adopting a higher level of assurance for authenticating and authorizing users.

As noted earlier, most UW System institutions operate a decentralized IT operation. Decentralization makes it challenging to adapt the same password standards across an entire campus. UW institutions also run other applications that require separate log-in user identifications and passwords. Institution staff reported that rather than memorizing a complex network password and all other passwords, especially when these passwords must be changed periodically, faculty, staff, and students tend to write the passwords down and to post them where they are easily accessible. This practice defeats the purpose of requiring strong passwords. A number of CIOs reported that their UW institutions are moving toward a single sign-on for all applications to reduce the number of passwords.

## **Physical Access to Data Centers and Network Equipment**

Another layer of computer security is the physical safeguards to protect against unauthorized access to facilities that house computer equipment. We discussed with staff physical security measures the institutions implemented. We also toured data centers at some UW institutions we visited.

UW institutions use a combination of measures to secure their data centers. The facilities are locked and only a limited number of IT staff and campus individuals have access to these facilities. Some institutions use electronic devices to log individual entry into and exit out of the facilities. Surveillance cameras are also installed to monitor all entries to and exits from the facilities and movement within the facilities. We detected many of these security measures implemented at the data centers we toured. None of the UW institutions we visited reported a successful break-in into their facilities within the last two years.

While data center managers and central IT network administrators we interviewed were confident in the safeguards implemented for the data centers, they expressed concerns about access to wiring closets and servers at various university departments. At some UW institutions with older buildings, the wiring closets also serve as janitorial closets. Campus staff noted that

separating janitorial and wiring closets may require funding through the capital project process. If so, institutional, System Administration, and State Building Commission involvement would be needed, and advance planning would be required. Central IT staff also indicated that they did not know how some departmental servers were physically secured.

The nature of security threats keeps changing.<sup>13, 14, 15</sup> Previously, worms and viruses were intended to disrupt networks. Recently, worms and viruses were meant to extract personal information. Early hackers were mostly individuals who wanted to experiment with their newfound hacking skills or to gain notoriety. Today hackers are sophisticated professionals, and according to the Computer Emergency Response Team (CERT) Coordination Center, part of a research and development center funded by the U.S. Government and charged with coordinating communication among security experts during security emergencies, some may be part of organized crime, seeking financial gains from the personal data they can access. Furthermore, networks change frequently. Thus, vulnerability assessments need to be completed on a periodic basis.

Since we did not perform technical assessments of the hardware and software UW institutions implemented and the access controls UW institutions put in place, we cannot comment on their adequacy and effectiveness for protecting computer networks and the data stored in these networks. However, UW institutions are in the best position to determine what their needs are and what security risks they can tolerate. Thus, ***we recommend that all UW System institutions perform periodic vulnerability assessments of their networks, including security hardware and software, passwords, and access to data centers and departmental servers, and mitigate the identified risks accordingly.***

While the technical assessments of UW networks are best performed by individuals with the appropriate expertise, assessing the effectiveness of some controls and procedures aimed at protecting computer networks and data might be performed by UW institutions' internal auditors. The assessment could be done in collaboration with campus IT staff, with assistance from staff experts at other UW institutions, or with external consultants. Institutional internal auditors can also assist with ongoing monitoring compliance with controls and procedures.

## **IT USER EDUCATION**

Computer users play a significant role in security, and IT experts agree that people are the greatest source of IT security problems. Statistics show that the majority of security breaches are caused by insiders.<sup>16</sup> Many insider breaches were the result of employees who were not aware of security threats. According to EDUCAUSE Center for Applied Research (ECAR), "continual security education is likely one of the most cost effective and important defensive strategies an

<sup>13</sup> Sieberg, Daniel. Hackers shift focus to financial gain. *CNN.com*, December 12, 2006, <<http://www.cnn.com/2005/TECH/internet/09/26/identity.hacker/index.html>>.

<sup>14</sup> William, Martyn. Security threat changing, says Symantec CEO. *Security.itworld.com*, December 12, 2006, <<http://security.itworld.com/4337/061103securitythreat/pfindex.html>>.

<sup>15</sup> Kvavik and Voloudakis. (See reference #12.)

<sup>16</sup> Gordon, Loeb, Lucyshyn, and Richardson. (See reference #11.)

institution can make.”<sup>17</sup> Furthermore, the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act (GLBA) require security awareness training for employees and management.

The UW System employs more than 38,000 faculty and staff and enrolled approximately 170,000 students in the 2006-07 academic year. Each faculty member, staff member, and student is a potential computer user and, therefore, is a potential contributor to the computer security problem if they are not aware of security threats. We reviewed computer security education programs that are aimed at increasing the campus computer users’ awareness about computer security.

UW institutions have offered varying degrees of security awareness education for their campus computer users. Offering information about security on institution websites is common. UW institutions have also developed flyers and posters and sent e-mails to users about specific computer security issues. Information provided covers issues such as passwords, patches, data storage, virus and spyware alerts, anti-virus protection, anti-spyware, phishing (an attempt to acquire private information by masquerading as an established and legitimate entity), and vulnerabilities associated with social networking sites, such as MySpace and Facebook. Figure 1 shows a sample of the type of information UW institutions provide to faculty, staff, and students.

**Figure 1: Sample of Information Provided to UW Computer Users on Security.**



Source: UW-Whitewater website (<http://www.uww.edu/security/>)

<sup>17</sup> Kravik and Voloudakis. (See reference #12.)

In general, we noted a more coordinated plan and effort in recent years to educate computer users at UW institutions with dedicated security offices or staff. In addition to information posted on institutional websites, UW-Madison, Milwaukee, Stevens Point, and Whitewater have also done formal presentations on security to various faculty, staff, and student groups on their campuses. UW-Milwaukee produced a kit on compact disc for students. The kit includes free anti-spyware and anti-virus software and other information about safe and secure computing. UW-Madison's security education strategy for faculty and staff has been to begin with IT staff and then expand the education to faculty and staff in other areas. CIOs we interviewed generally agreed that their institutions need to offer more security educational programs to students, faculty, and staff.

Educational awareness is designed to change behavior or to enforce good security practices. To be effective, basic information about computer security must be provided to all users and provided on an ongoing basis. The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce that supplies industry, academia, and government with standard reference materials, lists information that should be provided in a computer security education program. Some of the topics include:

- password usage and management, including creation, frequency of changes, and protection;
- protection from viruses, worms, Trojan horses, and other malicious codes;
- policy and implications of noncompliance;
- e-mail attachments;
- incident reporting and response;
- use of encryption and the transmission of sensitive/confidential information over the Internet;
- laptop computer security;
- personally owned systems and software at work;
- desktop security, such as use of screensavers, restricting visitors' view of information on the screen, and limited access to systems; and
- concerns regarding confidential information.

Since security education and awareness programs are critical to ensure that users are aware of threats and follow good computer security practices, ***we recommend that UW System institutions assess their education programs for computer users to ensure the programs cover information that is essential for safe and secure IT usage.***

To ensure that all users receive the information, mandating computer security training could be an option. Some universities, such as Virginia Tech and Oklahoma State University, and government agencies, including the Federal Deposit Insurance Corporation and the National Institutes of Health, made computer security education mandatory for students, staff, and faculty. The training is offered online and at the users' convenience.

## **CONCLUSION**

Threats to university networks and data stored on these networks are real, and colleges and universities, including UW institutions, have experienced security incidents. Protecting

computer networks and data is a complex task that is enhanced by a comprehensive information security program. Although this review is not a computer security audit, we determined that UW institutions have put considerable efforts into protecting university computer networks and confidential data. UW institutions have put various access controls in place; developed a wide range of policies; assigned staff resources to computer security; and provided education to faculty, staff, and students to increase their awareness of safe computing practices. However, protecting computer networks and data is a never ending process. With the increasing and changing nature of threats, UW institutions will need to increase attention to securing their computer networks and confidential data, to mitigate threats to UW computer networks and private data. We have recommended that all UW System institutions:

- designate a computer security officer position that has computer security as its primary responsibility and that requires the necessary computer security skills and competencies;
- develop an institutional policy that identifies the specific types of data that need additional protection;
- develop formal, written institutional policies and procedures on incident response;
- perform periodic vulnerability assessments of their networks, including security hardware and software, passwords, and access to data centers and departmental servers, and mitigate the identified risks accordingly; and
- assess their education programs for computer users to ensure the programs cover information that is essential for safe and secure IT usage.

## **Appendix 1**

### **Board of Regents Policy Document (RPD) 25-3 Policy on Use of University Information Technology Resources**

**(Formerly RPD 97-2)**

In accordance with its mission to disseminate and extend knowledge, to foster the free exchange of ideas, and to provide effective support for its teaching, research, and public service functions, it is the policy of the University of Wisconsin System to afford broad access to information technology resources <sup>1</sup> for university <sup>2</sup> students, faculty, and staff for use in fulfilling the university's missions, and for appropriate university-related activities.

#### **Access by Individuals**

Access to information technology resources carries with it the responsibility for ensuring that the use of these resources is primarily for university purposes and university-related activities, and for maintaining the integrity and security of the university's computing facilities. In the interest of making the use of information technology resources a natural part of the day-to-day work of all members of the university community, incidental personal use is tolerated. However, one should use non-university sources of e-mail, internet access, and other information technology services for activities of an extensive or recurring nature that are not related to university purposes. For the security of the information technology system, individuals having access to information technology resources must take reasonable care to ensure that unauthorized persons are not able to use their access to the system.

#### **Dissemination of Information and Official Documents**

Information technology resources are a dynamic mechanism for the free exchange of knowledge, and it is desirable for the university to foster the robust dialogue that results from the use of the resource, and to encourage students, faculty, and staff to participate in that dialogue. Those exchanges that reflect the ideas, comments, and opinions of individual members of the university community must, however, be distinguished from those that represent the official positions, programs and activities of the university. Students, faculty and staff using information technology resources for purposes of exchanging, publishing, or circulating official university documents <sup>3</sup> must follow institutional requirements concerning appropriate content and style.

The university is not responsible for the content of documents, exchanges or messages, including links to other information locations on the internet or world wide web, that reflect only the personal ideas, comments, and opinions of individual members of the university community, even where they are published or otherwise circulated to the public at large by means of university information technology resources.

#### **Inter-institutional Cooperation**

During times when they are away from the University of Wisconsin Institution where they are enrolled, students may benefit from the ability to use the information technology resources of another University of Wisconsin campus. To the extent possible with available resources, each University of Wisconsin System Institution should allow access to its information technology

resources by students taking distance education and other courses from other University of Wisconsin System Institutions.

### **Limitations on the Availability of Information Technology Resources**

The university's information technology resources are, by nature, finite. All members of the university community must recognize that certain uses of university information technology resources may be limited for reasons related to the capacity or security of the university's information technology systems, or as required for fulfilling the university's primary teaching, research, and public service missions.

### **Privacy and Confidentiality of Electronic Documents**

No information technology resources can absolutely guarantee the privacy or confidentiality of electronic documents. University of Wisconsin Institutions should, however, take reasonable precautions to protect electronic documents containing private and confidential information, and to assure persons using university information technology resources to transmit e-mail or electronic documents that the university will not seek access to their messages or documents except where necessary to:

1. Meet the requirements of the Wisconsin Public Records Law, or other statutes, laws, or regulations <sup>4</sup>;
2. Protect the integrity of the university's information technology resources, and the rights and other property of the university;
3. Allow system administrators to perform routine maintenance and operations, and respond to emergency situations; or
4. Protect the rights of individuals working in collaborative situations where information and files are shared.

University of Wisconsin System Institutions may choose to establish more detailed procedures for determining when access to electronic documents will be sought by the institution. As encryption products become more readily available, institutions may also wish to make them available to information technology users as appropriate to protect privacy interests.

### **Other Limitations on Use of Information Technology Resources**

In addition to the general principles set forth in this policy, the use of information technology resources may be affected by a number of other legal and ethical principles. While it is not possible to list all potentially applicable laws and regulations, the following are particularly likely to have implications for the use of university information technology resources:

1. Ethical standards of conduct for the appropriate use of one's university position and university resources are established for faculty and academic staff in Chapter UWS 8, Wisconsin Administrative Code, and for classified staff in Chapter ER-MRS 24, Wisconsin Administrative Code.
2. Chapters UWS 14 and 17, Wisconsin Administrative Code, establish standards and disciplinary processes relating to academic and nonacademic misconduct by students, including prohibitions on disruption of university activities, damage to university facilities, harassment, and similar matters.
3. Chapter UWS 18, Wisconsin Administrative Code, governs conduct on university lands, and applies to all members of the university community. Chapter UWS 21, Wisconsin Administrative Code, regulates the use of university facilities.

4. Section 943.70, Wisconsin Statutes, defines and prohibits certain computer crimes.
5. Chapter 11, Wisconsin Statutes, restricts the use of state facilities for political activities by state employees.
6. The federal copyright law applies to materials published or circulated through the use of computing resources.
7. The federal Family Educational Rights and Privacy Act restricts access to personally identifiable information from students' education records. Students, faculty and staff are responsible for understanding and observing these and all other applicable policies, regulations and laws in connection with their use of the university's information technology resources.

### **University of Wisconsin System Institution Responsibilities**

In order to assist members of the university community in fulfilling their responsibilities with respect to use of information technology resources, each University of Wisconsin Institution shall disseminate this policy, together with guidance, as to any specific campus policies affecting the use of information technology resources.

### **Failure to Comply with Information Technology Resource Policies**

Failure to adhere to the provisions of this policy may result in the suspension or loss of access to university information technology resources, appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff, or civil or criminal prosecution.

To preserve and protect the integrity of information technology resources, there may be circumstances where the university must immediately suspend or deny access to the resources. Should a student's access be suspended under these circumstances, the university shall inform the student immediately and shall afford the student an opportunity to respond. The university shall then determine whether disciplinary action under Chapter UWS 17, Wisconsin Administrative Code, or some alternative course of action, is warranted and shall follow the procedures established for such cases.

---

1 Information technology resources include computers, software, e-mail accounts, internet access, and similar computing tools.

2 "University" is used in this document to refer to the University of Wisconsin System and its institutions.

3 Official university documents are those which purport to speak for the university and its official programs and departments, such as policy documents, official forms, curriculum information, institutional statistics, and departmental home pages on the world-wide web.

4 The electronic records of university employees are subject to disclosure in accordance with the Wisconsin Public Records Law. Student records, including electronic documents, are protected against disclosure by the Family and Educational Rights and Privacy Act, which restricts access to personally identifiable information from students' education records.

History: Res. 7461 adopted 6/6/97.

## Appendix 2

### Security Hardware and Software Implemented By Businesses, Governmental Agencies, and Institutions of Higher Education

Hardware or Software	CSI/FBI Survey (N=616)	EDUCAUSE Survey (N=492)
Firewalls	98%	Perimeter – 89%; Interior – 80%
Anti-virus software	97%	Not specifically included in survey.
Anti-spyware software	79%	Not specifically included in survey.
Server-based access control list	70%	Not specifically included in survey.
Intrusion Detection System	69%	63%
Encryption	Transmission – 63% Storage – 48%	Transmission – 68% Storage – 27%
Intrusion Prevention System	45%	56%
Log management software	41%	60%
Application-level firewall	39%	57%
Smart card/one-time password token	38%	Not specifically included in survey.
Forensics tools	38%	Not specifically included in survey.
Public key infrastructure	36%	Without pin – 8% With pin – 7%
Specialized wireless security system	32%	Not specifically included in survey.
Endpoint security client software	31%	Not specifically included in survey.
Biometrics	20%	5%
Other	4%	Not specifically included in survey.
Virtual Private Network	Not specifically included in the survey.	85%
Centralized data backup system	Not specifically included in survey.	87%
Enterprise directory	Not specifically included in survey.	83%
Active filtering	Not specifically included in survey.	64%
Digital certificate	Not specifically included in survey.	59%
Security standards for application or system development	Not specifically included in survey.	51%
Electronic signature	Not specifically included in survey.	18%
Shibboleth (a web-based identity and access management technology)	Not specifically included in survey.	8%

Sources: Computer Security Institute and EDUCAUSE websites