

## **INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY**

### **1.0 INTRODUCTION**

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, electronic mail, WWW browsing, and access to any network resource, are the property of the University of Wisconsin-Stout (UW-Stout). These systems are to be used for academic and business purposes in serving the interests of the university and of our students and employees in the course of normal operations. Electronic mail (email) services are provided to the students, staff and faculty of UW-Stout in support of the teaching, learning and research mission of the University and the administrative functions to carry out that mission.

### **2.0 STATEMENT OF POLICY**

It is the University's position that the integrity and functionality of its information technology resources are directly impacted by the activities of its end users. The University must therefore both inform upon and require responsible computing practices from the members of the UW-Stout community. This policy applies to employees, students, contractors and consultants. This policy applies to all equipment that is owned or leased by UW-Stout.

The purpose of this policy is to outline the acceptable use of information technology at UW-Stout. Inappropriate use exposes UW-Stout to risks such as virus attacks, compromise of network systems, and disclosure of confidential data, services, and legal issues.

#### **2.1 Security and Proprietary Information**

2.1.1 The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by university. Examples of confidential information include, but are not limited to: university strategies, competitor sensitive, trade secrets, specifications, customer lists, and research. Employees should take all necessary steps to prevent unauthorized access to this information.

2.1.2 Passwords must be kept secure and confidential

2.1.3 All laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at a reasonable time or by logging-off when the host will be unattended.

2.1.4 All hosts used by the employee that are connected to the UW-Stout Internet/Intranet/Extranet, whether owned by the employee or UW-Stout, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy (see Appendix 2 for Guidelines for Wireless Communications).

#### **2.2 General Use and Ownership**

2.2.1 While UW-Stout's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the university systems remains the property of UW-Stout. Because of the need to protect UW-Stout's network, management cannot guarantee the confidentiality of information stored on any network device belonging to UW-Stout.

2.2.2 Employees and students are responsible for exercising good judgment regarding the reasonableness of personal use.

2.2.3 For security and network maintenance purposes, authorized individuals within UW-Stout may monitor equipment, systems and network traffic at any time.

UW-Stout reserves the right to audit networks and systems on a periodic basis to ensure compliance with the above statements.

### 2.3 Unacceptable Use

Under no circumstances is an employee or student of UW-Stout authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UW-Stout owned resources. (See Appendix 1 for List of Unacceptable Activities)

## **3.0 IMPLEMENTATION OF POLICY**

Telecommunications and Networking will make available and promote all information technology policies in an electronic format available through the World Wide Web and will implement whenever possible electronic means for the monitoring and enforcement of all information technology policies.

Use of the electronic media provided by UW-Stout is a privilege that offers a wealth of information and resources for research. Where it is available, this resource is offered to staff, students, and other patrons at no cost. In order to maintain the privilege, users agree to learn and comply with all of the provisions of this policy.

## **4.0 DEFINITIONS**

### **Term Definition**

Chain or email letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Email	All electronic mail communications and associated attachments transmitted or received
Forwarded email	Email resent from an internal network to an outside point
Extranet	Private network that uses Internet protocols to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses
Firmware	Computer program that is embedded in a hardware device.
Host	A computer connected to the network
Intranet	Private network that uses Internet protocols to securely share part of an organization's information or operations with its employees
PDA	Personal Digital Assistant (PDA) is a handheld computer used as mobile phones, web browsers, or portable media players
Public records	All writings made, maintained, or kept by the University for use in the exercise of functions.
Sensitive information	Information is considered sensitive if it can be damaging to UW-Stout or its customers reputation or market standing
Spam	Unauthorized and/or unsolicited electronic mass mailings
Unauthorized disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside UW-Stout, who do not have a need to know that information.
Virus Warning	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

### **Appendices**

1. List of unacceptable activities
2. Guidelines for Wireless Communications

## Appendix 1

### List of Unacceptable Activities

The following activities are prohibited. This list is not all-inclusive but provides a framework for activities which fall into the category of unacceptable use. The Chief Information Officer (CIO) may exempt an employee from one or more of these restrictions.

#### Examples of Prohibited Activities Related to Email:

- a. Sending unsolicited email messages, including the sending of "junk mail" or other non-university advertising material to individuals who did not specifically request such material (email spam).
- b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- c. Unauthorized use, or forging, of email header information.
- d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- e. Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
- f. Use of unsolicited email originating from within UW-Stout's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by UW-Stout or connected via UW-Stout's network.
- g. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- h. Distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
- i. Employees may not use their campus email account to conduct non-University business transactions

#### Examples of Prohibited Activities Related to Software:

- a. Illegal duplication of or use of software
- b. Any use of installation of software that is in violation of the applicable license agreement
- c. Acceptance of unlicensed software from any third party
- d. Installation of University-licensed software on a personally-owned, leased or otherwise ineligible computer except when expressly allowed by the applicable license agreement
- e. Employees may not use campus-licensed software to conduct non-University business or produce non-University content for compensation

#### Examples of other Prohibited Activities:

- a. Violations of the rights of any person or university or other entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UW-Stout
- b. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC)
- c. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question
- d. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, etc.).
- e. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home
- f. Using a UW-Stout computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction
- g. Making fraudulent offers of products, items, or services originating from any UW-Stout account

- h. Employees and students may not tamper with, modify, or extend University network services. This applies to all network wiring, data jacks, and related hardware, network or Internet services. Personal wireless access points, which would in effect extend the network and therefore potentially provide wireless connectivity to others, are prohibited
- i. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- j. Port scanning or security scanning
- k. Executing any form of network monitoring which will intercept data not intended for the student's or employee's host, unless this activity is a part of their normal job/duty
- l. Circumventing user authentication or security of any host, network or account
- m. Interfering with or denying service to any user other than the employee's or student's host (for example, denial of service attack)
- n. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's network session via any means, locally or via the Internet/Intranet/Extranet
- o. Providing information about, or lists of, UW-Stout students and employees to parties outside UW-Stout

## **Appendix 2.**

### Guidelines for Wireless Communications

This appendix specifies the conditions that wireless infrastructure devices must satisfy to connect to the UW-Stout network or reside on a UW-Stout site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

Only those wireless infrastructure devices that meet the standards specified in UW-Stout Policy 09-66, or are granted an exception by the Director of Telecommunications and Networking, are approved for connectivity to a UW-Stout network. Wireless data services are provided to the students, staff and faculty of UW-Stout in support of the teaching, learning, and research mission of the University and the administrative functions to carry out that mission. UW-Stout grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

All wireless infrastructure devices that reside at a UW-Stout site and connect to the UW-Stout campus network, or provide access to information classified as UW-Stout Confidential or UW-Stout Restricted must:

- a. Be installed, supported, and maintained by Telecommunications & Networking.
- b. Use UW-Stout approved authentication protocols and infrastructure.
- c. Use UW-Stout approved encryption protocols when applicable.
- d. Possess a Media Access Control address (MAC) that can be registered and tracked.
- e. Not interfere with wireless access deployments maintained by other support organizations.