1.0 Overview

Though there are a number of reasons to provide an individual network access, some of the common reasons are granting access to faculty and students to support educational activities and granting access to employees performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the university network. This policy explains how university information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the individual is asked additionally to use common sense when using university resources. Questions on what constitutes acceptable use can be directed to an individual’s supervisor or to the help desk.

2.0 Purpose

Since inappropriate use of university systems exposes the university to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of university information technology resources for the protection of all parties involved.

3.0 Scope

The scope of this policy includes any and all use of university IT resources, including but not limited to, computer systems, email, the network, and the university Internet connections.

Any faculty, student, employee, vendor, guest, or other individuals utilizing any university technology resources is required to abide by the requirements outlined in the university’s acceptable use policy. Use of university resources constitutes an individual’s acceptance of the terms outlined in the acceptable use policy.

4.0 Policy

4.1 E-mail Use
Personal usage of the university email systems by faculty and staff is only permitted on an incidental basis.
• The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
• Individuals are prohibited from forging email header information or attempting to impersonate another person.
• Email is an insecure method of communication, and thus information that is considered confidential or critical to the university may not be sent via email, regardless of the recipient, without proper encryption.
• Individuals should not open email attachments from unknown senders, or when such attachments are unexpected.
• Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that detailed information about the use of email may be covered in the university’s Email Policy.

4.2 Confidentiality
Confidential data must not be A) shared or disclosed in any manner to non-employees of the university without specific, written, regulatory authority, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

4.3 Network Access
The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her authorized activities or job function. Existence of access capabilities does not imply permission to use this access.

4.4 Unacceptable Use
The following actions shall constitute unacceptable use of the university network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The individual may not use the university network and/or systems to:

• Engage in activity that is illegal under local, state, federal, or international law.
• Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the university.
• Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying,
University of Wisconsin-Platteville

Acceptable Use Policy
Published: 01/26/2015

Section of: University Security Policies
Target Audience: Faculty, Staff, Students, and Guests

PUBLIC Page 3 of 8

insulting, threatening, obscene or otherwise inappropriate messages or media.
• Engage in activities that cause an invasion of privacy.
• Engage in activities that cause disruption to the university environment/workplace or create a hostile environment/workplace.
• Make fraudulent offers for products or services.
• Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
• Install or distribute unlicensed or "pirated" software.
• Reveal personal or network passwords to others, including family, friends, or other members of the household when accessing university resources from home or remote locations.

4.5 Blogging and Social Networking
Blogging and social networking by university’s employees are subject to the terms of this policy, whether performed from the university network or from personal systems. Blogging and social networking are allowed from the university computer network provided that A) it is done in a professional and responsible manner, B) confidential data is not disclosed, C) it does not impact an employee’s job performance, and D) no information detrimental to the university is published. The individual assumes all risks associated with blogging and/or social networking.

4.6 Instant Messaging
Instant messaging is allowed such that it follows guidelines on disclosure of confidential data and does not negatively impact an employee’s job function.

4.7 Overuse
Actions detrimental to the computer network or other university resources, or that negatively impact job performance are not permitted.

4.8 Web Browsing
The Internet is a global network of interconnected computers of which the university has very little control. In addition, academic requirements necessitate the university to maintain a relatively open network. The individual should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The university is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

4.9 Personal Internet Use
The University recognizes that the Internet can be a tool that is useful for academic, personal, and professional purposes. Personal usage of university computer systems to access the Internet is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the university or on an employee’s job performance.

4.10 Copyright Infringement
The University’s computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which an individual has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

4.11 Peer-to-Peer File Sharing
Peer-to-Peer (P2P) networking is allowed as long as illegal and/or copyrighted materials are not downloaded or shared, and as long as it does not negatively impact the computer network or an employee’s job performance.

4.12 Streaming Media
Streaming media can use a great deal of network resources and thus must be used carefully. Reasonable use of streaming media is permitted as long as it does not negatively impact the computer network or an employee’s job performance. Specific questions on acceptable streaming media can be directed to the help desk or an employee’s supervisor.

4.13 Monitoring and Privacy
The University is subject to the State of Wisconsin open records laws. Individuals should not have an expectation of privacy when using the university’s network or university resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The university reserves the right to monitor any and all use of the computer network. To ensure compliance with university policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.14 Political Activity
Political activities by university faculty and staff that utilize university resources, detrimentally
impact their employee job performance, or which are performed using their position within the university, are prohibited. Political activities by students are permitted, but are subject to the restrictions on university resource use. Details of what is prohibited and what is allowed regarding political activity for students and employees is outlined in the UW-System “Guidance on Political Campaign Activities at University of Wisconsin System Institutions” URL: https://www.wisconsin.edu/government-relations/guidance-on-political-campaign-activities-at-university-of-wisconsin-system-institutions/

4.15 Bandwidth Usage
Excessive use of university bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low university-wide usage.

4.16 Personal Usage
Personal usage of university computer systems by students and guests is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the university. Incidental personal usage of the university computer systems by faculty and staff is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the university or on the employee’s job performance.

4.17 Remote Desktop Access
Use of remote desktop software and/or services is allowable as long as it is provided by the university. Remote access to the network must conform to the university’s Remote Access Policy.

4.18 Circumvention of Security
Using any university provided or personal computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

4.19 Use for Illegal Activities
No university provided or personal systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
• Unauthorized Packet Sniffing
• Unauthorized Packet Spoofing
• Unauthorized Denial of Service
• Unauthorized Wireless Hacking
• Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
• Acts of Terrorism
• Identity Theft
• Spying
• Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues
• Downloading, storing, or distributing copyrighted material

The university will take all necessary steps to report and prosecute any violations of this policy.

4.20 Non-University-Owned Equipment
Non-university-provided equipment utilizing the university network or accessing university resources is required to utilize up-to-date anti-virus software and patching and must comply with all university policies such as appropriate network use, data protection, etc.

4.21 Personal Storage Media
The university does not restrict the use personal storage media, which includes but is not limited to: USB or flash drives, external hard drives, personal music/media players, and CD/DVD writers, on the university network provided that guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the university network. Use of personal storage media must conform to the university’s Mobile Device Policy.

4.22 Software Installation
Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. The university expects individuals to use discretion when installing software on computers utilizing the university network. Individuals may be restricted from installing software on university-provided equipment to minimize risk exposure to the university environment. When in doubt, the best course of action is not to install the software in question. Questions around appropriate software use may be directed to the helpdesk or the university purchasing office.
4.23 Reporting of Security Incident
If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the university Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains university information.
- Loss or theft of ID badge, key, or keycard that would grant access to confidential data or restricted areas.
- Any attempt by a person to obtain an individual’s password over the telephone or by email.
- Any other suspicious event that may impact the university’s information security.

Individuals should treat a suspected security incident as confidential information, and report the incident only to his or her supervisor and the UW-Platteville Information Security Officer. Individuals must not withhold information relating to a security incident or interfere with an investigation.

4.24 Applicability of Other Policies
This document is part of the university’s cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Individuals utilizing the university’s resources are also governed by the UW-System Administration Board of Regents policy 25-3, “Policies On Use of University Information Technology Resources.” The text of the full policy can be read on the UW-System Administration policy website: [http://www.uwsa.edu/bor/policies/rdp/rdp25-3.htm](http://www.uwsa.edu/bor/policies/rdp/rdp25-3.htm). UW-Platteville’s acceptable use policy is a supplement to the UW-System Administration Board of Regents policy, in situations where the two may conflict, the Board of Regents policy supersedes the UW-Platteville policy.

5.0 Enforcement
This policy will be enforced by the Assistant Vice Chancellor for Information Technology in consultation with Human Resources and/or the Dean of Students. Violations may result in disciplinary action, which, for students is outlined in Chapter 14 and Chapter 17 of the student conduct agreement and for all individuals may include suspension, restriction of access, or more
severe penalties up to and including termination of employment. Where illegal activities or theft of university property (physical or intellectual) are suspected, the university may report such activities to the applicable authorities.

### 6.0 Definitions

**Blogging:** The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

**Instant Messaging:** A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

**Peer-to-Peer (P2P) File Sharing:** A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

**Remote Desktop Access:** Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

**Streaming Media:** Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

### 7.0 Revision History

Revision 1.0, 01/26/2015