Policy Name: Acceptable Use Policy for Computing Resources

Responsible Department: Information Technology

Approving Body: Policy Committee

Approved Date: Tuesday, December 15, 2014

**Purpose:**

The purpose of this policy is to outline the acceptable use of computer equipment, internet and technical resources at WNMU. These rules are in place to protect the employee and WNMU. Inappropriate use exposes WNMU and individuals alike to risks including virus attacks, compromise of network systems and services, and legal issues.

**Policy:**

**Overview**

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to WNMU’s established culture of openness, trust and integrity. Academic Freedom is a core value for Information Technology. Information Technology is committed to protecting that freedom as well as WNMU’s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of WNMU. These systems are to be used for business purposes in serving the interests of the company and the interests of our customers. Our business is education and our customers are the students.

Effective security is a team effort involving the participation and support of every WNMU employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

**Scope**

This policy applies to employees, contractors, consultants, temporaries, and other workers at WNMU including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by WNMU.
Terms

Users
A person who makes use of university technology resources.

Information Technology

Policy

A. General Use and Ownership
1. While WNMU’s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of WNMU. Because of the need to protect WNMU’s network, management cannot guarantee the confidentiality of information stored on any network device belonging to WNMU.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. WNMU adheres to a high standard for technical support. To ensure this, any device, software or other technology that is to be supported by Information Technology must first be verified by Information Technology before purchase.
4. For security and network maintenance purposes, authorized individuals within WNMU may monitor equipment, systems and network traffic at any time.
5. WNMU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

B. Security and Proprietary Information
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 corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Department level passwords should be changed quarterly, user level passwords should be changed every six months.
3. Postings by employees from a WNMU email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of WNMU, unless posting is in the course of business duties.
4. All hosts used by the employee that are connected to the WNMU Internet/Intranet/Extranet, whether owned by the employee or WNMU, shall be kept up
to date with operating system patches, security updates and service packs.

5. All hosts used by the employee that are connected to the WNMU Internet/Intranet/Extranet, whether owned by the employee or WNMU, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

6. Employees must use good sense and caution when confidence scams, “phishing” attempts or other social-engineered attacks are used against WNMU.

7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of WNMU authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing WNMU-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. If there is any uncertainty to the legality of an action, employees should consult their supervisor or manager.

A. System and Network Activities
The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company 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 WNMU.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which WNMU or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Copying and or/distributing university software to non-university personnel or systems is also illegal, be it physical media or electronic download/shares.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Introduction of any network peripheral (e.g., wireless access points, routers, switches, etc) without notification and consultation of Information Technology.

6. 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.

7. Using a WNMU 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.
8. Using a WNMU computing asset to actively engage in transmitting material that is
pornographic, hate-mongering, slander or inciting violence of any sort.
9. 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.
10. Port scanning or security scanning is expressly prohibited unless prior notification with
Information Technology is made.
11. Executing any form of network monitoring which will intercept data not intended for the
employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for
example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to
interfere with, or disable, a user's terminal session, via any means, locally or via the
Internet/Intranet/Extranet.
15. Providing information about, or lists of, WNMU employees to parties outside WNMU.

B. Email and Communications Activities
1. Sending unsolicited email messages, including the sending of "junk mail" or other
advertising material to individuals who did not specifically request such material (email
spam).
2. Any form of harassment via email, telephone or paging, whether through language,
frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. 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.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within WNMU's networks of other
Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service
hosted by WNMU or connected via WNMU's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet
ewsgroups (newsgroup spam).

Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and
including termination of employment.

Revision History
Procedures:
None