Policy: New Students and Staffs IS Orientation and Training

1.0 Overview

Knowledge of departmental Information Systems resources is a critical component to how people interact with others and how they perform in everyday work environments. With an increase in requirements for computer data safety (EPHI, HIPAA) and the general nature of technology growth, having initial computer training and orientation when entering the job is needed. This will increase productivity, familiarize staff with IS personnel, and generally educate which reduces future increased loads on IT staff.

2.0 Purpose

This policy helps establish a base level of knowledge and understanding of specific department level information system applications, network usage, tools, resources, polices, and guidelines.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Dept of Medphysics facility, has access to the Dept of Medphysics network, or stores any non-public information.

4.0 Policy

4.1 General

New student defined above will be required to have scheduled meeting with IS staff within one week of their official start date detailing the following items:

A. Login, logout actions, and changing passwords.

B. Navigating, saving, and retrieving files to network drives

C. General usage including sending, checking email, saving drafts, working with calendars and creating vacation reminders.

D. A general outline of the department's public and private website.

E. Any additional items the Student might need to carry out their daily work.

5.0 Enforcement

Any faculty or student member found to have violated this policy may be subject to removal of network.

6.0 Definitions

EPHI Electronic Protected Health Information

HIPAA Health Insurance Portability and Accountability Act

Appropriate Use Policy

Policy for Appropriate Use of University of Wisconsin-Madison Information Technology Resources

Access to electronic mail, the Internet, databases, computers and other information technology (IT) resources is essential to the mission of the UW-Madison (to create, integrate, transfer and apply knowledge), and the achievement of excellence requires their effective use by all members of the University community. Use of information technology must be consistent with the University's mission and with its role as a public agency. Each member of the University community is expected to protect the integrity of these resources and to know and adhere to University rules, regulations and guidelines for their appropriate use. Regulations that govern personal conduct and use of University facilities* also apply to the use of IT resources. In addition, the following policy applies more specifically to use of IT resources:

General Guidelines

1. Access to University IT resources is a privilege granted to members of the University community which carries with it the responsibility to use them for University related activities, exercising common sense and civility.

2. **Individual Responsibility**

   Authorization for use of IT facilities is provided to each individual for his or her own use. No person may use an authorization which belongs to someone else. In many cases the University has obtained access to these resources exclusively for the use of members of the University community.

3. **Security**

   The protection of University IT resources depends heavily on each user's careful handling of "keys" to these resources, since any account can serve as an entry point for theft, damage or unauthorized use. Users must protect the confidentiality of their personal identification codes and passwords and are expected to exercise reasonable care to ensure that others cannot use their accounts.

4. **Intellectual Property**

   Illegal downloading, distribution, copying of copyrighted materials or other activities that violate copyright law are strictly prohibited.

5. **"Hacking"**

   Persons may not obtain or use--or attempt to obtain or use--passwords, IP addresses or other network codes that have not been assigned to them as individuals or authorized for their use as University employees. Persons may not obtain--or attempt to obtain--unauthorized access to computer accounts, software, files, or any other University IT resources.

6. **Malicious Activity**

   Persons may not alter or intentionally damage software or data belonging to someone else or interfere with another person's authorized access to IT resources. Users may not intentionally disrupt or damage University computers or networks in any way.

7. **Impersonation and Anonymity**

   Users of University IT resources may not send electronic messages with the sender's identity forged or send anonymous messages unless the recipient has agreed to receive anonymous messages.

8. **Commercial, Political and Non-University Activities**

   Persons may not use University IT resources to sell or solicit sales for any goods, services or contributions unless such use conforms to UW-Madison rules and regulations governing the use of University resources. University employees may not use these resources to support the nomination of any person for political office or to influence a vote in any election or referendum. No one may use University IT resources to represent the interests of any non-University group or organization unless authorized by an appropriate University department.

9. **De Minimis Usage**

   In the interest of making the use of IT resources a natural part of the day-to-day learning and 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 IT services for activities of an extensive nature that are not related to University purposes.

10. **State and Federal Laws**
    Persons may not use University computing facilities to violate state or federal laws.

* as published in the University of Wisconsin System Administrative Code and UW-Madison policies. For example, disruption of University activities, damage to facilities, physical threat, theft or harassment as described in UWS 17 and 18; student academic misconduct in UWS 14; selling, peddling and soliciting in UWS 18; and ethical standards for use of facilities by faculty and staff in UWS 8.

Violation of University rules governing appropriate use of IT resources may result in loss of access privileges, University disciplinary action, and/or criminal prosecution.

Medphysics IT Office