

Understanding Your Information Security Responsibilities

This document outlines the information security responsibilities that come with your work at the University. You must review this security awareness information and University Policy #6104: Acceptable Use of Information Technology Resources and Systems and return the included Information Security Awareness Agreement form on page 3.

Information security is everyone's responsibility and we all have specific responsibilities to protect IT resources, systems and data. You should always be aware of and follow the policies and procedures of the University and your department. Many of these requirements are also great advice for protecting personal information and computers in your role as a student.

Protect sensitive information and IT resources and systems:

Sensitive information – information, in print and electronic form, about yourself, others and the University that needs protection from unauthorized disclosure, unauthorized changes and/or unavailability.

IT resources and systems – the networks, programs, databases, computing devices, etc. that must be operational and must contain accurate information for the university to fulfill its responsibilities.

Your responsibilities:

- Maintain the confidentiality of information that you have access or exposure to in the course of your work.
- View only the information you are asked to view. Make only the changes you are authorized by your supervisor to make.
- Protect University IT resources and systems from malware and unauthorized access or changes.
- Report any concerns and ask any questions regarding information security to your supervisor.

In order to fulfill your duties, you may be provided additional IT resource and system access. Any additional access will be assigned through standard University procedures. Use this access only as directed by your supervisor.

Protect computers from malware:

Malware is software that can damage a computer or IT system. Examples of malware include viruses, worms, Trojan horses, spyware, adware, bots, etc. University computers have malware protection software installed that should always be in operation and you should also ensure that any other computer you use has malware protection.

Your responsibilities:

- Be suspicious of all links, attachments or downloads that accompany e-mails or other electronic messages.
- Be aware that web sites may be infected with malware.
- Report to your supervisor any University computer behaving irregularly which you believe may be the result of malware.

Handle data securely:

The University has specific requirements for handling data.

Your responsibilities:

- Ask your supervisor:
 1. Where documents should be stored.
 2. How the data may be transmitted.
 3. How data storage media, such as hard drives, USBs or CDs, should be used.
- Know the procedures of disposing of sensitive information, such as through shredding of physical documents or returning electronic data storage media to your supervisor for proper disposal.

Protect your password:

University password requirements ensure that all campus passwords meet minimum standards for length and complexity and ensure that passwords are changed regularly.

Your responsibilities:

- Keep your password private.
 - Don't tell it to anyone. (IITS will never ask for it and neither should anyone else).
 - Don't let anyone else use your password.

Respect intellectual property rights:

Policy #6104: Acceptable Use of Information Technology Resources and Systems policy requires you to respect copyrights such as those copyrights protecting music, movies and software.

Your responsibilities:

- Protect copyrights (and prevent malware) by not installing software on University computers.
- Realize that music, movie and software trade associations do contact the University regarding copyright violations and we do follow up.

Use wireless access wisely:

Because of the speed, reliability and security of wired access you should use wired access as opposed to wireless access when possible.

Your responsibilities:

- Work with your supervisor to determine if wireless is appropriate for the work you are doing.

Report security incidents:

Security incidents are suspicious or abnormal events that occur on IT resources or systems such as unauthorized access to a system, unauthorized modifications to data or misuse of IT systems.

Your responsibilities:

- Report any concerns about security to your supervisor.

Policy 6104
**ACCEPTABLE USE OF INFORMATION TECHNOLOGY
RESOURCES AND SYSTEMS**

I. PURPOSE

The purpose of this policy is to establish parameters for the use of Longwood information technology (IT) resources and systems.

II. DEFINITION

IT Resources and Systems: IT resources and systems include all computers, workstations, peripherals, networks, communications devices, switches, software programs and systems, as well as all related devices, hardware and software owned by Longwood University, covered under contract by the Commonwealth of Virginia or that are the responsibility of Longwood University through agreements with Longwood departments or employees.

III. POLICY

This policy covers all activities involving these IT resources and systems and applies to all individuals using these IT resources and systems. This policy does not cover activities solely involving personal property, but does cover activities which involve the use of personal property connected to or communicating with Longwood University IT resources and systems.

A. Intent of IT Resources and Systems: IT resources and systems are provided at Longwood and shall be used solely to support the mission of the University and its related academic, administrative and service activities. Activities involving Longwood's IT resources and systems must be in accord with the Longwood University Honor Code, the Student Handbook, the Faculty Policies and Procedures Manual and the Administrative Policies and Procedures Manual, as well as, relevant local, state, federal and international laws and regulations.

B. Privileged Systems: Use of Longwood IT resources and systems is a privilege granted to individuals by the University and is restricted to the specific authorities granted. Access to the use of discrete IT resources and systems shall be explicitly granted by the owner of the IT resource or system or his or her designee.

C. Acceptable Use: For use to be acceptable, it must demonstrate respect for:

1. The intent of the individual authorities granted the user;
2. The usage privileges of other authorized users;
3. The rights of others to privacy;
4. Intellectual property rights (e.g., as reflected in licenses and copyrights);

5. Ownership, confidentiality, integrity and availability of systems and data;
6. System mechanisms designed to limit, monitor and/or record use or access (Longwood University IT resources and systems activity are routinely monitored and recorded by technical support staff.);
7. Current network topology and configuration; and
8. Individuals' rights to be free of intimidation, harassment and unwarranted annoyance.

D. Responsibility to Investigate Possible Misuse:

1. The University reserves the right to monitor, access and disclose all data created, sent, received, processed or stored on any University IT resource or system with or without cause.
2. When there is reasonable suspicion of misuse the University has the responsibility to investigate. Such investigations will only be undertaken by the CIO or his or her designee with the permission of the President or his or her designee.
3. The CIO or his or her designee has the right to temporarily suspend or modify access privileges.

E. Internal Audit Reviews: In the course of its work, Internal Audit has full and complete direct access to all University books and records (manual and electronic) relevant to the subject of review. All documents and information given to Internal Audit during their work will be handled in the same prudent manner that the University expects of the employees normally accountable for them.

IV. ENFORCEMENT

The University regards any violation of this policy as a serious offense. Violators of this policy are subject to appropriate disciplinary action such as prescribed in the Longwood University Honor Code, the Student Handbook, the Faculty Policies and Procedures Manual and the Administrative Policies and Procedures Manual, in addition to possible cancellation of IT resources and systems access privileges. Users of IT systems and resources at Longwood are subject to all applicable local, state and federal statutes. This policy does not preclude prosecution of criminal and civil cases under relevant local, state, federal and international laws and regulations.

Revised and approved by the Board of Visitors, September 7, 2002.
Revised and approved by the Board of Visitors, September 10, 2005.
Revised and approved by the Board of Visitors, September 14, 2006.
Revised and approved by the Board of Visitors, September 12, 2008.

Information Security Awareness Agreement

Return this completed form to the Academic and Career Advising Center.

Student Name: _____

Supervisor Name: _____

Department: _____

By signing and returning this form you are acknowledging that:

- (1) You have reviewed the document “Understanding Your Information Security Responsibilities” and University Policy #6104: Acceptable Use of Information Technology Resources and Systems.

- (2) You agree to follow the guidance provided in each of these documents.

Student Signature

Date