

Information Technology Security

I. Abstract

This module explains the University's commitment to a safe and secure computing and networking environment. It is incumbent upon each of the 50,000 faculty, members, staff and students who comprise our network community to take reasonable precautions to ensure that the University's technology resources can continue to work appropriately, free from malicious hacking, computer viruses and intruder attacks.

II. Helpful Contact Information

University Technology Services
("UTS")
PC 531
Ext. 7-2284

Information Technology
Security Office
PC 534A
Ext. 7-1366

III. Rules of the Road

- a. The University is committed to a safe and secure computing and networking environment. As such, the University's policies and procedures provide numerous administrative, technical and physical safeguards aimed at ensuring the availability, integrity and confidentiality of the information/data created, received and maintained by the University.
- b. Members of the University Community who have access to sensitive/confidential data, should be familiar with the University's Data Stewardship Procedure available at: <http://policies.fiu.edu/files/560.pdf>
 - i. This procedure provides that all highly sensitive data must be accessed by way of a unique name or number for identifying and tracking user identity.
 - ii. If stored electronically, it must be encrypted using a minimum of 128 bit encryption.
- c. In order to promote information technology security, the University's Information Technology Security Office offers departmental and online IT Security training. The materials that follow below have been prepared by the University Information Technology Security Office.
- d. When using the University's information technology services, please:
 - i. Visit <http://security.fiu.edu> for training guidelines and policy statement and sign up for IT security training.
 - ii. Be sure to read some Peer 2 Peer (P2P) guidelines before you use P2P Applications. Visit <http://security.fiu.edu/policies.htm> to find out what materials are permissible to share via P2P and to be aware of the serious penalties for violating copyright laws that may result from misuse of P2P programs.

Information Technology Security

- iii. FIU's network resources cannot be used for commercial or solicitation purposes, to violate copyright laws, to harass or defraud another, or to damage or disrupt individual computers or networks. In addition, subject to very limited and narrow exceptions, Florida law prohibits the use of University resources (e.g. information technology resources including e-mail systems) for state lobbying purposes.
- iv. Keep your PC secure:
 1. In order for the University to secure its computing environment, the University requires that all employees who work with a university laptop or desktop computer that relies on the Windows® operating system must either join the UTS Active Directory Domain, or become a member of their department's Active Directory which meets required minimum security standards.
 2. Active Directory manages the following requirements for connecting to the FIU network infrastructure:
 - Virus Protection
 - Locking Screen Saver
 - Local Firewall
 - System Patch Management
 3. You are still the key to completing the IT security strategy. Below are standard security practices that you are required to follow:
 - a. Use strong passwords. Choose passwords that are difficult or impossible to guess, but easy to remember.
 - b. Make regular backups of critical data. Imagine losing research material or papers that you spent many hours working on. This can be avoided by making sure you frequently back up the data on your PC.
 - c. Do not leave computers online when not in use, either shut them off or physically disconnect them from the Internet connection.
 - d. Do not leave your computer running and accessible to strangers. If you have to step away, lock it.
 - e. Do not open e-mail attachments from strangers. Be suspicious of an unexpected e-mail attachment even from someone you know because it may have been sent without that person's knowledge from a virus-infected machine.
- v. Network Access: You may have your access to FIU's network resources revoked for the following reasons:
 1. Unpatched systems. Computer systems on the FIU network that do not have necessary security patches (fixes) installed in a timely manner.

Information Technology Security

2. Compromised computer systems. Computer systems that have been intruded upon and/or set up to execute commands or programs at the direction of an unauthorized individual or agent (a hacker).
 3. Computer virus proliferation. Your computer system is infected with a computer virus or worm that propagates via FIU network and system resources.
 4. Copyright infringement. Violation of established copyright laws.
 5. Denial of service attack. A direct attempt to prevent legitimate users of a service from using that service.
 6. Hacking. Knowingly accessing another's computer or network without explicit authorization.
- e. For more information, please visit the Information Technology Security Office Web site at <http://security.fiu.edu> .