

The policies listed in this document are only an abbreviated list of the Information Resource Management Technology Policies. For the complete list of policies go to: <http://www.fau.edu/irm/techpolicies.htm> .

PREFACE

IRM technology policy exists in addition to all other legally binding documents to guide the conduct of Florida Atlantic University users as it pertains to technology resources. It is not intended to replace in part or in whole pertinent Florida or federal law such as the Computer Crimes Act, Chapter 815 of the Florida Statutes; the Public Records Law, Chapter 119 of the Florida Statutes; the Digital Millennium Copyright Act, <http://www.loc.gov/copyright/legislation/dmca.pdf> ; the Computer Fraud and Abuse Act of 1986; the Computer Abuse Amendments Act of 1994 or obscenity and child pornography laws. Furthermore, displaying or sending obscene or pornographic materials to those who do not wish to see them is also a violation of the University's sexual harassment policy, http://www.fau.edu/divdept/equalop/sex_harr.htm .

All users agree to comply with IRM policies and with applicable state and federal laws dealing with appropriate, responsible and ethical use of information technology. It is not the responsibility of IRM to ensure user compliance with IRM technology policy. It is the responsibility of the user to be aware of the existing policies and to adhere to their guidelines. Non-compliance is a serious breach of University standards and may result in legal and/or disciplinary action.

1. Network Management and Security

Bandwidth

Bandwidth, or the transmission capacity, of our network hardware is a finite resource all electronic information on our network must share. This information can be referred to as network traffic and organized into different traffic queues. Each network switch and router is configured with a priority associated with each traffic queue. These rules are maintained in a central server within IRM and distributed to all switches and routers on the FAU network. IRM staff reserves the right to develop the rules governing these priorities based on the relative importance of different applications, users, and groups in conjunction with available resources.

Hacking for malicious purposes

Hacking is the interference with or unauthorized access to any computer or computer network. This may or may not reflect malicious intent. Specific examples of 'malicious hacking' include:

- Any attempt to gain root or system administrator privileges on any FAU network machine or equipment, without permission
- Any attempt to gain unauthorized access to files, equipment or accounts
- Any attempt to do anything that results in interruption of any service to FAU customers
- Any use of chat robots
- Any attempted use of password cracking software
- Circumventing IRM approved firewalls
- Specific software attacks, including 'Smurf attacks' and 'Ping of Death'
- Any attempt to access or change system files, without permission
- Any unauthorized attempt to store user files outside their predefined areas.
- Installation or attempted use of SUID programs of any type, without permission
- Any attempt to do these things through FAU network, even if the attempt is aimed outside our network
- Use of the Napster or other shared-multimedia application software such as Scour

Malicious hacking may compromise system availability, data integrity or both. IRM will, to the fullest extent allowed by law, seek legal action against any individual(s), organization(s) and or company(s) that directly or indirectly utilizes our network (or causes it to be used) for any practice that we consider to be hacking with malicious intent.

Port scanning and sniffing

Port scanning and sniffing are legitimate, diagnostic activities that IRM engages in to maintain the availability and performance of the University network at acceptable levels. Both, however, can be misused for malicious purposes to gain access to sensitive information traveling on our network or to find weaknesses in computer systems that will allow access to unauthorized individuals.

Port scanning is only permitted by IRM and/or appropriate law enforcement agencies for detecting security holes on University workstations and servers. If a system connected to our network is found to have a security hole, the owner will be notified. If the security issue is not addressed within an agreed upon period of time, the system will be removed from the network without further notice.

Sniffing is only permitted by IRM to identify the source of bad data on the network. This data can cause unacceptable performance degradations and inaccessibility of network resources. Once a source is identified, IRM staff will take any necessary action to prevent further transmission of such data.

Network infrastructure

IRM must authorize in writing all networking equipment in use and connected to the FAU network prior to being physically attached to that network. IRM staff will manage all authorized networking equipment. Any unauthorized equipment of any kind found attached to the network will be disconnected immediately and without notification to the owner.

Network address assignment and Dynamic Host Configuration Protocol (DHCP)

Each device attached to a network must have a unique address associated with it. The assignment and accurate maintenance of these addresses is key to a healthy, functioning network. Management of these functions is solely the responsibility of IRM. DHCP is a readily available method by which address assignment can be automated. No unauthorized use of DHCP will be permitted. Any unauthorized device acting as a DHCP server will be disconnected immediately without prior notification to the owner.

Wireless network

IRM is solely responsible for the design, operation and management of the FAU wireless network. The FAU wireless network operates within the unlicensed 2.4 GHz radio frequency range. Wireless equipment includes but is not limited to wireless transceivers, or Access Points, directly connected to the wired network and wireless antennas which amplify radio frequency signals. Antennas are in compliance with FCC 15.203 and University safety regulations. Any tampering with any of these devices will result in appropriate disciplinary action. Any unauthorized wireless device found connected to the FAU wired network will be disconnected immediately without notification to the owner.

Anonymous FTP sites

All users intending to implement anonymous FTP on any workstation or server must notify IRM of this intention. Users must not offer licensed or illegal software on their site. Users must not allow anonymous users connecting to their site write access. Any FTP site on the University network found in non-compliance with these restrictions will be disconnected immediately.

Firewalls

Firewalls are software barriers to unsolicited or malicious network activity as well as being a barrier to unauthorized users of a network. IRM maintains its own firewall as an added protection against malicious use of our network. Personal firewalls must be approved by IRM in writing for individual servers and/or

workstations. It must be shown that they will not interfere with overall network function and performance as determined by IRM.

Electronic mail (email) and spam

All email created and sent in the pursuit of official University business will be considered public record and it is the responsibility of each user to become familiar with all aspects of Florida's Public Records Law, Chapter 119 of the Florida Statutes. Non-compliance with this law will result in disciplinary action.

The following actions are expressly forbidden.

- Forgery (or attempted forgery) of electronic mail messages
- Attempts to read, delete, copy, or modify the electronic mail of others
- Attempts at sending harassing, obscene, and/or other threatening e-mail to another user
- Attempts at sending spam

Spam is any unsolicited email message sent to a large number of people. Typically this includes cases where:

- The recipient did not request the message.
- The recipient does not know the sender.
- In newsgroups, a message is posted that is not appropriate to the topic of the newsgroup. Newsgroup postings that offer services or products are considered spam, unless they can be documented as a response to a legitimate inquiry in that same newsgroup, and if they are appropriate to the topic of that newsgroup.
- Bulk mailing lists are used to send unsolicited marketing or sales information.

If everyone with a product to sell or an opinion to voice sends an email to hundreds or thousands of people, the network will be overwhelmed and become unusable. Therefore, IRM does not condone the practice of spamming, i.e. sending spam as identified above. IRM will, to the fullest extent allowed by law, seek legal action against any individual(s), organization(s) and or company(s) that knowingly or otherwise directly or indirectly utilizes the FAU network (or causes it to be used) for any practice that sends out mass unsolicited e-mail.

It is the responsibility of each user to respect the finite capacity of the computing resources made available by IRM and to limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Each user account is assigned specific resources for use by email messages. It is the user's responsibility to stay within these resource boundaries. IRM reserves the right to delete email when it exceeds the limits of

said resources. Furthermore the size of email messages and/or attachments is limited to 5 MB. Messages exceeding the 5 MB limit rapidly consume system and user resources interfering with the delivery of all email. As a result messages and/or attachments greater than 5 MB will be refused by the mail system.

IRM encourages the use of electronic mail and respects the privacy of others. IRM does not wish to inspect or monitor electronic mail routinely or be the arbiter of its contents. Nonetheless, IRM may access electronic mail and data stored on the University's network of computers for the following purposes:

- troubleshooting hardware and software problems
- preventing unauthorized access and system misuse
- investigating reports of a violation of University policy or local, state or federal law
- complying with legal requests for information
- rerouting or disposing of undeliverable mail

IRM will need the approval of the Associate Provost of IRM or his appointee to access specific mail and data for the above specified purposes. The extent of the access will be limited to what is reasonably necessary to acquire the necessary information.

2. Student computing privileges

All student users of IRM computing resources must have a current, valid FAU email account and photo-id card. Access to IRM computing resources will be denied to students that do not have both of the afore-mentioned items. Student users must also agree to abide by the computing policies set forth by IRM when given an FAU email account. Students that violate these policies will be reported to the Dean of their respective college and their computing privileges will be suspended or revoked depending on the severity of the violation. All illegal activities will be reported to the University Police Department and prosecuted to the fullest extent of the law. ***Computer use for a student is a privilege, NOT a right.***

Student housing

The Department of Housing and Residential Life will ensure network connectivity within the residence halls and student apartments. However, FAU students are bound by IRM technology policies within the confines of student residences on any or all FAU campuses as they are within any University owned structure.