

# FLORIDA ATLANTIC UNIVERSITY

777 GLADES ROAD  
P.O. BOX 3091  
BOCA RATON, FLORIDA 33431-0991

**TO:** The Florida Atlantic University Community

**FROM:** Jeffrey Schilit, PhD  
Associate Provost and Chief Information Officer  
Information Resource Management

**DATE:** September 06, 2006

**RE:** IRM Technology Policy update

Beginning in April 2000, IRM began the lengthy process of collecting, reviewing and building, where necessary, policies intended to define IRM's role in innovation and support of technology for the FAU community. Networking and technology resources are central, indispensable tools in education, research and administration. As a result the need for a comprehensive body of policies became critical.

To this end the IRM Policy Development Committee was formed and formally charged on April 19, 2000. The committee was composed of representatives from each functional area within IRM, bringing a broad, comprehensive perspective to the task ahead. Once a working list of policy areas was defined, the group divided into subcommittees to explore each in depth. Current laws were reviewed along with the policies of our peer and sister institutions. IRM Directors then brought the individual policies together and after extensive review and further additions, the document was deemed ready for distribution.

This policy document is viewed by IRM as an ever-evolving process that will be updated and added to as appropriate and/or needed to reflect new technologies and policy changes.

The staff of IRM hopes the FAU community will benefit from this collection of policies. Our intent is to educate and inform as well as guide faculty, administration, staff and students in the responsible, ethical use of technology resources at FAU.

April 2000	Original document
July 24, 2004	First revision
November 7, 2005	Second revision
September 6, 2006	Third revision

# **INFORMATION RESOURCE MANAGEMENT TECHNOLOGY POLICIES**

**February 6, 2007**

Developed by the Division of Information Resource Management

Jeffrey Schilit, Associate Provost IRM and CIO  
Elise Angiolillo, Director, Communications Services Infrastructure  
Mehran Basiratmand, Chief Technology Officer, Director, Enterprise Computing Services  
Joanne Julia, Director, Northern Computing Services  
Molly Munro, Director, Online Client Services  
Denise Payeur, Director, Fiscal Management  
Susy Quiggle, Director, Broward Computing Services  
Douglas Trabert, Director, University Learning Resources  
Paul Wright, Director, University Administrative Systems

## **ACKNOWLEDGEMENTS**

To all individuals from within IRM who either served on the IRM Policy Development Committee or contributed to the collected policies herein and to all members of the University community who contributed their time and expertise in the compilation of these policies, thank you. Without your cooperation and teamwork this document would not have been possible.

IRM Policy Development Committee, 2000

Miriam Crisman, Chairperson  
Keith Adderly  
Wayne Bullock  
Mark DeHass  
Joe Diliddo  
Joe Guest  
Ivette Puga  
Carol Sashi  
Anthony Scott  
Dianne Thibodeau  
Doug Trabert  
Cary Winters  
Paul Wright

A special thank you to Wilfredo Hernandez, University Police, for invaluable advice from a law enforcement perspective.

## 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\\_har.htm](http://www.fau.edu/divdept/equalop/sex_har.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.

These policies are applicable to all IRM resources and are global in scope. It may become necessary for individual departments and/or colleges to define in more detail the limitations on their internal computing resources by further refining the policies stated here. No department and/or college may, however, override the guidelines and restrictions contained within IRM technology policy. A committee appointed by the Associate Provost of IRM will review the policies each year to ensure current applicability to technology resources across all campuses.

## POLICY DEVELOPMENT

A University shall be governed by known and consistent policies and procedures, over which the members of the community have some consultative influence. The policies of a University should be clear, fair and widely understood. Since discussion must precede action, the question of how policy is developed and how it is communicated are closely linked.

Additions to and revisions of the policies of this University are acts of the President; the President may delegate authority for policy and action in certain areas to others. Members of the University community should be consulted on matters of policy that fall within their concern. Those with responsibility for policy will consult those concerned through the institutions of academic governance.

A policy administrator, designated for a given policy area, is responsible for

implementation of policies in that area. The administrator will also be responsible for periodic review of policies. Proposals to review policies may come from any source and the administrator is responsible for consultation on proposals to change policy.

## **AUTHORITY**

Empowerment for this set of IRM policies and guidelines comes from Florida Atlantic University, Office of the University Provost and Chief Academic Officer and is approved by the President of the University. The Associate Provost for IRM is charged with upholding all IRM policies and guidelines.

## **REVISION AND MAINTENANCE PROCESSES**

All policies are subject to review, revision or elimination. As noted, additions to and revisions of the policies of the University are acts of the President. The President may delegate authority for policy and action in certain areas to others.

Revision and maintenance of current policies should be accomplished through one of the following processes.

(A) Ad Hoc Review---A director or staff member may initiate a review of a policy if in their judgment the policy is in conflict with other existing policy or policies or has become outdated. A departmental director and an appointed panel of departmental staff members will conduct a formal review of the policy in question.

(B) Continuous Renewal---The policy defined here and all policies developed and approved as attached shall be assessed annually from the effective date to determine continuing effectiveness and appropriateness. The process of policy development may be assessed before that time as a function of substantive change concurrent with infrastructure growth.

## **DEFINITIONS**

Policy - statements of principals or guiding actions defining acceptable behavior and individual responsibilities; a statement of values or intent that provides a basis for consistent decision-making and resource allocation. Policies have widespread application, change infrequently, are expressed in broad terms and address fundamental operational issues.

Procedure - series of steps followed in chronological order that implement stated policy. Procedures have narrow applications, change frequently, are stated in detail and describe process.

## **ACCESS TO POLICY**

Official FAU-IRM policy shall be made available to the University community electronically. Printed copies of official policy shall also be available through the Offices of the University Provost, the Associate Provost for IRM and IRM Directors.

<b>I. Technology Allocation in Construction Budgets</b> .....	8
A. Building Wiring Facilities.....	8
B. Conduit and Cable Facilities.....	8
<b>II. IRM Supported Software and Hardware</b> .....	8
A. Administrative Data Systems.....	8
B. Banner.....	9
C. OASIS.....	9
D. MyFAU.....	9
E. FAUNetID/Username.....	9
F. Access to Computers for People with Disabilities.....	10
G. Servers Secured with SSL.....	11
H. Desktop Standards.....	11
<b>III. Help Desk Operation</b> .....	11
<b>IV. Service Level Agreements for Technical Support Staff</b> .....	12
<b>V. Acceptable Use and Ownership of Information Technology Resources</b>	12
A. Space Utilization Policy.....	13
B. Computing Equipment.....	13
C. Software.....	13
D. Access to Computing Resources.....	14
E. User Accounts.....	15
F. Copyright.....	15
G. Intellectual Property Rights.....	15
H. Web Pages.....	15
I. Audiovisual and Multimedia Equipment.....	15
J. Videoconferencing Facilities.....	16
K. Telecommunications Equipment.....	17
L. Phone Mail.....	18
M. Calling Cards.....	19
N. Blackberry.....	19
O. Cellular Phones.....	19
P. Network Storage Space.....	19
<b>VI. Network Management and Security</b> .....	20
A. Bandwidth.....	20
B. Hacking For Malicious Purposes.....	21
C. Port Scanning and Sniffing.....	21
D. Network Infrastructure and Communications Closets.....	22
E. Network Address Assignment and Dynamic Host Configuration Protocol (DHCP).....	22
F. Domain Name Registration.....	23
G. Wireless Network.....	23
H. Anonymous FTP Sites.....	24
I. Peer to Peer (P2P) File Sharing and Software Piracy.....	24
J. Firewalls.....	25
K. Electronic Mail (Email) and Spam.....	25
L. Email Accounts.....	27

M. Distribution Lists.....	28
N. World Wide Web .....	28
O. Commercial Web Use .....	28
P. WISE Privacy Policy .....	28
<b>VII. Student Computing Privileges .....</b>	<b>29</b>
A. Student Computer Labs – Software.....	29
B. Instructional Computer Labs – Scheduling .....	30
C. Student Housing.....	30
<b>VIII. Peer Campus Computing Support .....</b>	<b>31</b>
<b>IX. Emergency Preparedness and Disaster Recovery .....</b>	<b>31</b>
A. Emergency Use of the FAU Mail System .....	31
B. Emergency Changes to Voice Greetings And Web Pages .....	32
C. FAU Emergency Policy .....	32
D. Equipment .....	32
E. Backups.....	32
F. Student Computer Lab Operations .....	33
G. IRM Disaster Recovery Plan .....	33
<b>X. Instructional Technology Support and Distributed Learning .....</b>	<b>34</b>
A. Distance Learning.....	34
B. Instructional Design and Development .....	35
C. Television and Video Production Services .....	35
D. Television Engineering .....	35
<b>XI. Miscellaneous Issues .....</b>	<b>36</b>
A. Health Insurance Portability and Accountability Act of 1996.....	36
B. Grant Recovery for Computing Services .....	36
<b>References .....</b>	<b>37</b>

# INFORMATION RESOURCE MANAGEMENT TECHNOLOGY POLICIES

## **I. Technology Allocation in Construction Budgets**

### A. Building Wiring Facilities

The University has adopted a standard for communications wiring to support current and future communication requirements within its buildings. (Refer to IRM Communication Infrastructure Specification.) This standard shall be used by all agencies and staff offices in the planning and design of all office buildings, including the wiring of new and the upgrading of existing buildings. This applies to both FAU and leased FAU buildings. IRM's Communications Services Infrastructure (CSI) shall review all plans for communication wiring and must approve installation of wire or other communication media. IRM's University Learning Resources shall review the installation of presentation and teleconferencing equipment wiring in all new construction.

### B. Conduit and Cable Facilities

The conduit and cable system for all voice and data communications on all FAU campuses is managed by IRM's, CSI. IRM staff maintains records of all voice and data communication infrastructure on all campuses, including outside cable and conduit as well as in building wiring up to the individual jack. No department may use the University's inside wire plant for voice communication without the consent of IRM, and payment of applicable one-time and/or monthly charges. No department may use, reconfigure or re-terminate the University outside communication plant under any circumstances without the express written consent of the IRM Associate Provost.

## **II. IRM Supported Software and Hardware**

### A. Administrative Data Systems

On behalf of the University community, IRM supports the major administrative applications residing on mainframes located in State of Florida data centers. IRM operates and maintains administrative servers, locally, running Windows Operating Systems, UNIX and Oracle for University-wide applications. The responsibility for support, operation, and maintenance of departmental computing resources remains with the individual department.

IRM also maintains computer equipment acting as repositories for University Databases. (Refer to Presidential Memorandum #84, <http://www.fau.edu/admin/pm/84.htm> ) University Data Bases contain official data

used to report the operations of the University. Only the University Data Base Administrator has the authority to endorse changes to the University Data Bases and/or release any data contained therein.

IRM has the responsibility to ensure the maximization of existing and future University administrative data systems. To this end, IRM is authorized to coordinate, direct, and approve the design, purchase, implementation and utilization of additional University administrative data systems resources across campuses, colleges and departments. (Refer to Presidential Memorandum #90, <http://www.fau.edu/admin/pm/90.htm> .)

### B. Banner

SCT Banner is a fully integrated, enterprise system that provides authorized users with financial, personnel, payroll, purchasing, and student information. IRM maintains the hardware and software systems while specific departmental areas are responsible for user support, application training, reports, access authorization, and data input.

### C. OASIS

OASIS is the **Owls Academic Student Information System**. OASIS is a comprehensive web resource available to all students, full or part-time, degree seeking or non-degree seeking. Students, faculty and staff may register, check grades, Search for courses, pay tuition and fees, check student records, review financial aid, and change their personal information number code (PIN). OASIS is available every day from 7:15am until 10:00pm. IRM supports the technical system and database while the Registrar's office maintains responsibility for user support, training, data input, and authorizing access. <https://oasis.fau.edu/>.

### D. MyFAU

MyFAU, <http://myfau.fau.edu/cp/home/loginf>, is a web based portal that provides centralized access to e-mail, electronic calendars, administrative services, course schedules, university announcements, and classroom tools. MyFAU is accessible to students, faculty and staff with a single username(faunetid) and password. IRM supports the hardware and software maintenance of MyFAU and is responsible for faculty and staff training. University departments are responsible for channel and/or tab content specific to their departments. Individual users may customize their own pages to reflect their needs.

### E. FAUNetID/Username

A FAUNetID is automatically generated for faculty and staff upon employment and students upon application to the University. Individuals will have the use of the account for as long as they maintain an official affiliation with the University.

Your assigned FAUNet ID is unique across all FAU campuses and serves as your login to many university computing and networking services. The FAUNet ID also determines your FAU email address. The format of the FAUNetID for faculty, staff and students is the first initial of the first name and up to seven letters of the last name. Faculty and staff may choose to have an alias composed of their first and last names. Examples of each are shown below. For more information regarding email policies refer to [Email and Spam](#) in Section VI.

**YourFAUNetID@fau.edu (Example: jdoe@fau.edu)**

**Alias format: firstname.lastname@fau.edu**

A FAUNet ID is automatically generated for students once they have applied to the University. One semester after graduation or after three successive semesters during which a student has not registered for a course, the account will be disabled. All student accounts are verified annually.

IRM provides a FAUNetID to all faculty and staff, including adjunct faculty during active employment. The account will be disabled immediately after employment is terminated and it will be removed from the system after 60 days. The sole exception to this refers to retired faculty accounts.

The original FAUNetID or username is not subject to change. The only exception to this would be if an individual has changed his or her name legally, through the judicial system. Legal name changes for faculty and staff must be recorded in the Department of Human Resources. Students must submit their name changes through a form on the OASIS Web. See the Personal Information section for more information and a link to the form. Requests for a faunetid change may be made at any time however the actual change will take place between semesters or at the discretion of IRM.

#### F. Access to Computers for People with Disabilities

In order for students with disabilities to be guaranteed equal access to technical resources they must be registered with the Office for Students with Disabilities (OSD). The students must register well in advance of obtaining the needed services. This will ensure that there is adequate time for their needs to be properly evaluated and appropriate services identified. Students with disabilities are obligated to use accommodations responsibly. IRM will coordinate with the OSD to ensure access to computer services. Faculty and staff should coordinate any special needs with their supervisors and the Help Desk to find reasonable accommodations to suit their special needs.

### G. Servers Secured with SSL

User offices that wish to secure a server through implementation of a Secured Socket Layer License for application processing should contact the IRM Help Desk. IRM will mediate the purchase of the SSL license, if necessary. Users should not purchase the license on their own. Coordination of the installation and support of the SSL license is the responsibility of IRM's Enterprise Computing Services.

### H. Desktop Standards

IRM has established standards for supported hardware and software. IRM personnel will support software and hardware purchased by departments and/or colleges if it complies with these standards and has a valid license in the case of a software application. The Purchasing Department will also assist users in acquiring hardware products supported by IRM at the time of purchase. For those hardware and software acquisitions not contained within these standards, users will be referred to product support lines, product manufacturers or the individual requiring the use of the product.

Support for past versions of supported software will be limited to the version immediately preceding the current version. Support for the oldest version will be phased out as support for the newest release becomes established. In addition, IRM maintains standard desktop configurations combining necessary applications, utilities and hardware allowing for timely and consistent user support. Software support is also limited to software installed on university owned equipment on university property. IRM hardware standards include minimum system requirements for these desktop configurations. Hardware that no longer meets the minimum system requirements of supported applications and their associated configurations will not be supported. (Refer to <http://www.fau.edu/irm/desktop/hardware.php> for supported hardware standards and to <http://www.fau.edu/irm/desktop/software.php> for supported software standards.)

It is also the intent of IRM to offer software support through problem resolution and software installations as well as through educating the user community in the use of supported applications. Information regarding available classes, class schedules, eligibility requirements and registration information can be found at <http://www.fau.edu/irm/training/>.

## **III. Help Desk Operation**

As the first level of support for IRM services, all calls for information or assistance are logged, monitored and routed by the IRM Help Desk. The Help Desk is available 24x7. All logged calls are assigned a ticket number for tracking

purposes. It is IRM's intent to resolve as many calls as possible at the Help Desk level of support. When other resources are required, Help Desk staff will route the call to the appropriate IRM staff for resolution.

Logged calls are given priorities based on the severity of the problem and the scope of its impact on the user community. Users are given the ticket numbers for any unresolved issues to facilitate further inquiries. For calls having top priority, responsible IRM staff will be contacted immediately to begin resolution. Once resolved, descriptions of the resolutions become a permanent part of the knowledge base employed by Help Desk staff as a reference for all future calls.

#### **IV. Service Level Agreements for Technical Support Staff**

To successfully meet user expectations in computing resources and services, IRM will establish Service Level Agreements (SLA) with appropriate departments, colleges and/or service units throughout the University and within IRM itself. In order to offer end-to-end quality of service guarantees, it is necessary that each party guarantee the availability and performance of each service component. Service level agreements will be developed as needed to provide these guarantees of availability, reliability and responsiveness. In this way, IRM services will be provided in a timely, efficient manner.

SLAs are binding documents stating non-compliance of agreement, fees if applicable, arbitration procedures, modification terms, reporting responsibilities, stated objectives and areas accountable for completion of any tasks necessary for compliance. All parties entering into a SLA with another service unit, department or college will be required to supply signature of their dean, director or an appointee. These agreements will be kept on file within IRM and reviewed for continued relevance, as need dictates.

#### **V. Acceptable Use and Ownership of Information Technology Resources**

The information technology resources provided and maintained by IRM are intended for university-related purposes including the support of the University's mission, its administrative functions and activities within the student community. Users shall have no expectations of privacy with respect to the use of such resources. IRM may access any and all information technology resources at any time in accordance with Section V.D. of this Information Resource Management Policy. Personal use of these University resources may be made on an incidental basis only and shall not consume a significant amount of those resources or interfere with the performance of University responsibilities. Further limits may be imposed upon personal use in accordance with normal supervisory or academic procedures concerning the use of University equipment. Appropriate use of computing resources includes respecting the privacy of other

users and their accounts, using only those resources you are authorized to use, respecting the finite capacity of these resources so as not to limit their accessibility by others and abstinence from using any of these resources for personal gain or commercial use not related to university business. Unauthorized and/or inappropriate use of these resources is prohibited and may result in disciplinary and/or legal action. Unauthorized or fraudulent use of university telecommunications resources can result in felony prosecution as provided for in state or federal law.

#### A. Space Utilization Policy

All IRM Rooms are for the sole use of Information Resource Management and approved Common/Inter-exchange Carriers with the following exceptions:

- **Parking Garages:** IRM rooms in parking garages may be used by other entities with IRM approval. If the room contains IRM equipment, the room will be partitioned and designed so that IRM equipment is not accessible to non-IRM employees.
- **Grandfathered Locations:** Shared locations that currently exist will remain intact unless the building is renovated at which time IRM will seek separate space.
- **Pass-Through IRM Rooms:** Rooms which are used only to provide cable access from one location to another will be considered by IRM for use by other entities. If use of the room is approved, the locks will be changed to allow non-IRM entities access only to the Room(s) in question.

#### B. Computing Equipment

IRM may require users of computing equipment to limit or refrain from specific uses of that equipment if their activities are destructive or interfere with university computing operations or resources. Individuals who require the use of university equipment at home must follow the procedure developed by the Office of the Controller, Property Management Department for taking university owned equipment off campus and complete the associated form, <http://www.fau.edu/admin/fiscal/controller/property/offcampus.pdf>. Computing equipment may include but is not limited to workstations, laptops, servers and network devices such as routers, patch panels and switches.

#### C. Software

Users are responsible for ensuring that all software installed on their desktop computers, departmental/college servers or remote storage areas is licensed and that it is used in support of university activities. The legality of at-home use of university owned software varies from application to application. To determine the licensing terms of site licensed software go to the Online Support Center at

<http://www.fau.edu/helpdesk> to request information or to search the knowledge base for answers. Violation of intellectual property laws and license agreements or malicious use of software is strictly prohibited.

Peer to peer file sharing applications enabling the exchange of files across the Internet and the FAU network will be permitted if they are used in support of the University's mission in teaching, research and community service. If the use of such software is found to violate the University's Intellectual Property Policy, the Digital Millennium Copyright Act, the Florida Computer Crimes Act or federal law the appropriate disciplinary and/or legal actions will be taken. If the operation of such software is found to interfere with the normal functioning of the FAU network, hinder network performance or compromise network security, IRM will notify the user and take necessary action. Refer to Peer to Peer File Sharing and Software Piracy in Section VI.

#### D. Access to Computing Resources

Users will be granted appropriate access to all computing resources necessary in conducting University business; however, users shall have no expectations of privacy with respect to the use of such resources. IRM may access any and all information technology resources at any time in accordance with this Section V.D. Personal use of these University resources may be made on an incidental basis only and shall not consume a significant amount of those resources or interfere with the performance of University responsibilities. Further limits may be imposed upon personal use in accordance with normal supervisory or academic procedures concerning the use of University equipment. Normal operation and maintenance of computing resources requires backups and caching of voice or data communications, logging of resource activity and monitoring of general usage patterns in addition to other activities necessary in providing service to the user community. IRM may specifically monitor activity and/or accounts of individuals without notice. Any monitoring, other than approved monitoring situations as defined in this Section V.D. will be authorized by the University President. Approved monitoring situations include but are not limited to the following:

- The user has voluntarily made his or her use of these resources accessible to the public by means of a web page, posting to a Usenet service, or similar display of activity in the public realm.
- It appears reasonably necessary to do so to protect the safety, integrity, security or functionality of any component of the University community or its computing resources.
- It appears reasonably necessary to do so to protect the University from liability.
- It appears reasonably likely that the user has violated or is violating federal or state law or any University regulation or policy, including without limitation, IRM computing policies.

- An account appears to be engaged in unusual or unusually excessive activity.
- It is required or permitted by law, specifically including without limitation the Florida Public Records Laws.

#### E. User Accounts

Refer to FAUNetID in Section II.

#### F. Copyright

IRM supports the Federal Standard for Copyright ( <http://www.loc.gov/copyright/> ) and Fair Use ( <http://www.copyright.gov/help/faq/faq-fairuse.html> ). Any copyrighted material appearing on University web sites must adhere to acceptable use policies or be supported by written permission from the owner of the copyrighted material.

#### G. Intellectual Property Rights

Compliance with the Intellectual Property policy as defined by the Office of the President is mandatory. Refer to <http://www.fau.edu/academic/provost/IPP.pdf>

#### H. Web Pages

The FAU WISE Server and other Web Servers on campus, promote the University and are vehicles which assist users in finding more information about Florida Atlantic University. Official university web pages should reflect the official business of the college, department, center or individuals who compose and maintain them. Faculty, staff and students maintaining individual web pages on the University WISE server should comply with the guidelines as indicated on the WISE developer site at <http://www.fau.edu/wise/>.

#### I. Audiovisual and Multimedia Equipment

IRM staff is responsible for supplying, maintaining, delivering and retrieving audiovisual equipment, including multimedia hardware and software, used in direct classroom instruction for credit courses, non-credit courses, seminars, workshops, conferences and administrative activities. Personal use is prohibited. It is also not permitted to remove any or all of the aforementioned items from university campuses without IRM approval. Charges are applicable to non-credit activities, student sponsored events, events where an admission charge or fee is collected and funded grant activities.

All requests for audiovisual or multimedia equipment must be accompanied with the appropriate FAU account number and submitted in writing 72 hours prior to the desired service date and time. No phone requests will be honored except in

emergency situations. Demonstration of proper equipment use is available as is consultation on technical concerns. Loan period limits are 14 calendar days for laptops and 7 calendar days for other audiovisual equipment.

All classrooms and teaching auditoriums are furnished with an overhead projector, television monitor, VCR and projection screen. Electronic equipment is locked to an audiovisual cart. Unauthorized use of or destructive behavior towards audiovisual or multimedia equipment is prohibited. Equipment examples include projectors, viewing screens, VCR players, laser disc players, microphones, CD players, laptops computers and televisions.

No smoking, food or drink is permitted in multimedia teaching auditoriums and videoconferencing rooms. Faculty must be present during the entire class session and ensure that no changes are made to equipment settings and cables. Faculty should attend training sessions on the use of these specialized rooms.

#### J. Videoconferencing Facilities

IRM's videoconferencing systems allow point-to-point and multi-point communication between FAU campuses or locations outside the University (with similar conferencing equipment). Videoconferencing is best defined as a fully interactive meeting or conference involving participants at two or more locations connected by electronic means with full motion video and high quality audio. The connection may be one-way video and two-way audio or two-way video and two-way audio. Two separate and distinct videoconferencing networks have been built. One network has been designated as the Academic System. This is to be used primarily for instructional and research purposes. The second network is for administrative purposes. The transmission mode for the videoconferencing process occurs either via telephone lines (H.320) or via the Internet (H.323) protocols.

IRM maintains and operates the networks over which all videoconferencing takes place. IRM staff will provide assistance with scheduling, operation, and support of the administrative videoconferencing network so long as the conference is booked three (3) business days in advance. Technical support cannot be guaranteed unless the conference is booked through IRM. IRM exclusively manages all aspects of the academic videoconferencing network.

All videoconferencing units that reside on FAU properties utilize the FAU computer network or Internet2 and will use academic or administrative videoconferencing rooms on FAU campuses. Videoconferencing units must be registered through IRM/ULR. The registration form must be submitted to the Associate Director of University Learning Resources - Global Management System at 7-2079. Only registered units will be allowed to schedule or connect to any videoconferencing network unit or location.

### *Videoconferencing Scheduling*

All use of the academic videoconferencing network and locations must be scheduled through ULR Videoconferencing Connectivity Management office, 7-3698. Scheduling decisions will be based on availability and priority, using the Provost's Memorandum on *Priority Scheduling for General Classrooms*. All academic videoconferencing rooms will have a designated contact person to assist in the scheduling process. The contact person will assist in the room setup, minor operational training for the user, and re-securing the room following the scheduled event.

Scheduling, for the administrative videoconferencing rooms, is the responsibility of the campus specific senior administrator or his/her designee.

Videoconferencing rooms on all FAU campuses are maintained and operated by IRM staff. IRM staff will assist in opening and preparing each room for each scheduled function and will secure the room afterwards. All such rooms will be kept locked when not in use. Staff for the operation of the administrative videoconferencing network will primarily fall within the province of campus administration. However, when asked or when appropriate, IRM will assume staffing responsibilities for this environment.

### *Maintenance and Repair of Videoconferencing Hardware*

The maintenance and repair of academic videoconferencing equipment and associated network hardware will be the responsibility of IRM technical staff. Maintenance and repair of the administrative videoconferencing equipment will be supervised by technical staff. Costs associated with the maintenance and repair of this equipment and supporting hardware will be the responsibility of the administrative videoconferencing network owner.

Maintenance and repair of videoconferencing equipment and supporting hardware not owned and operated by IRM will be the responsibility of the owner.

### K. Telecommunications Equipment

The telephones, voice communication switches and associated peripheral equipment are maintained by IRM's Communications Services Infrastructure is responsible for all aspects of university telephone systems at all campuses and other supported locations. CSI has been designated as the sole University point of contact for common carriers, other service providers, and voice and public network services.

### *Equipment Ownership*

Telecommunications equipment from the jack out is the responsibility of IRM.

This equipment includes line cords, telephone sets, modem lines, or other telecommunication terminals. This equipment is purchased by and leased to the end user's department. The design of the voice system software is proprietary and requires the use of authorized equipment only.

### *Equipment Maintenance*

Maintenance of all telephone lines and equipment is the responsibility of Communications Services Infrastructure within IRM. CSI will not move furniture, file cabinets, etc., to access telephone jacks or equipment.

### *Service Problems*

All telephone service problems must be called into the CSI Trouble line at 7-6333. The trouble line is checked throughout the working day and the normal restoration period should be no longer than 24 hours.

### *Financial Responsibility for Equipment and Services*

Each department is responsible for all charges for telecommunication services including, but not limited to the following:

- Activation costs for the line
- Monthly service charges for the line and it's associated features
- Maintenance of any equipment attached at the jack
- Charges for any user-caused damage to the jack, line or telephone system (as might be caused by faulty equipment or other electronic equipment connected to the jack)
- Lost or stolen phones
- Incoming collect calls accepted at the telephone set
- Local area calling charges, if applicable to the line
- Installation of voice and data cables

### L. Phone Mail

Users shall not send telecommunications messages the content of which is defamatory, or which constitutes breach of telecommunications security, or is in violation of University policies, Federal, State, or local laws.

Telecommunications messages intended for general distribution to all campus users shall be reviewed and approved in advance by the appropriate department head or appointee to determine that such information is suitable for general distribution.

### M. Calling Cards

Calling cards are available from the Fiscal Management Department within IRM. All charges incurred from their use will be billed to the requesting department on the monthly Telecommunication Services Statement. The requesting department is liable for all charges for any calls placed using that calling card. The individual to whom the calling card is issued is responsible for the security of the card.

### N. Blackberry

The Blackberry PDA functions as a cellular phone, wireless email client and web browser. Its use must be approved by department heads and IRM. Departments requesting Blackberry devices are liable for all charges or service fees and the individual to whom the Blackberry is issued, is responsible for the security of the phone. All users must comply with IRM policies dealing with appropriate, responsible and ethical use of technology.

### O. Cellular Phones

Each department requesting cellular service for the official business of the University must submit a request to IRM's Communications Services Infrastructure. All charges incurred for usage will be billed to the requesting department on the monthly Telecommunication Services Statement. The requesting department is liable for all charges for any calls placed, and the individual to whom the cellular phone is issued, is responsible for the security of the phone. Cell phone purchases and usage that are comprised of legitimate E&G expenditures shall not be eligible for payment through any Foundation account. Payment for cell phone service, using a qualified state plan, shall come from the appropriate E&G or Auxiliary account.

Changes to this policy will be determined by the University President, his/her designee, or a member of the FAU Senior Administration. Once this determination has been made, one of the individuals previously identified, or the Associate Vice President for University Advancement will convey to the IRM Associate Provost & CIO and the Director of Telecommunication Services/Project Management the modifications to be made.

### P. Network Storage Space

All faculty, staff and student users are allotted network storage space. Each individual is provided with a personal (home) directory. Colleges, departments and/or administrative groups must request network storage if they require it. It is the responsibility of each user to back up his or her files, however faculty and staff directories will be included in system-wide back ups. Access to user directories will be disabled once the user is no longer affiliated with the University. The contents of individual user directories will be deleted and the

directories removed under the same rules that apply to email accounts. (See Email Accounts policy under section VI.) Students are limited to 20 MB of file space. Faculty members are limited to 100 MB of file space.

*The use of this resource is only intended for data files that support the teaching, research and service missions of FAU. Any material stored for personal gain, commercial or frivolous use not related to university business is prohibited. Storing unlicensed software is prohibited. Storing copyrighted material without the permission of the copyright owner, except as allowed under copyright law, is prohibited. All violations of this policy will result in loss of privileges and disciplinary and/or legal action as appropriate.*

## **VI. Network Management and Security**

In the Information Age in which we live, management of network resources and the security of the University network are fundamental to the pursuit of the University's goals of academic excellence, increasing research activities and serving the needs of the surrounding communities. Network resources, accepted network behavior and their associated policies are defined as follows. IRM does not manage personally owned IT resources which include computers and other network-connected devices. Examples include, but are not limited to, personally owned laptops, computers and other devices used in classrooms and student housing.

IRM is responsible for all network access points used by unmanaged hosts, but is not responsible for the hosts themselves. IRM is responsible for identifying users responsible for a given port at any given time and must be able to initiate disruption of service to the user's FAUNetID and/or network address. IRM is responsible for coordinating the notification to the user and ensuring that the incident is resolved.

IRM security measures comply with all state and federal laws and university policies.

### A. 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 on 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.

## B. 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 the 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.

## C. Port Scanning and Sniffing

Port scanning and sniffing are legitimate, diagnostic activities that IRM engages in to maintain the availability and performance of the FAU 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.

#### D. Network Infrastructure and Communications Closets

The network infrastructure or hardware includes but is not limited to switches, hubs, routers, patch panels and network cable. Most of this equipment is housed within communications closets in university buildings on each campus. Only IRM authorized personnel will be allowed access to these communications closets and only IRM authorized personnel will be allowed access to the network equipment housed within these closets or elsewhere, where no closet is available.

In addition, 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.

#### E. 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 essential 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. Network addresses for university computing equipment are categorized as static; DHCP with registration and reservation; and DHCP open access.

*Static IP addresses* are most commonly assigned to desktop systems, servers, printers and networking equipment. Access from these devices to remote resources on the FAU network or Internet do not require user authentication. User authentication is handled at the application level as is the case for local system access, email or network file services.

*DHCP with registration and reservation* applies to mobile computers such as laptops in their preferred location. These addresses are reserved for a single system and require no authentication from a designated site. Individuals requiring the use of DHCP from a primary location must go to the Online Support Center at <http://www.fau.edu/helpdesk> to request this service.

*DHCP open access* address assignment refers to all devices, configured for

DHCP, connecting to the network from a network port that is not a preferred location. These systems will be assigned a network address dynamically. Anyone connecting to the Internet using this address configuration will be required to authenticate user ID and password initially and every four hours once connected.

#### F. Domain Name Registration

IRM staff is the only agent at FAU who can register a network address and domain name/host name to any network device before its installation on the FAU network. As with network addresses, domain names and host names must also be unique within subnets, the FAU network being composed of multiple subnets. *All requests for server and workstation domain names/host names and network addresses must go through IRM systems and networking staff.* When submitting a domain name registration request for a server a Dean, Director or his/her designee must approve the request. The request will then come before the IRM Network Advisory Committee. This committee in consultation with IRM systems and networking staff will review requests making certain requested domain names are appropriate, consistent with the mission of the University and in compliance with standard naming conventions. If the requested name is already in use, the requestor must choose another following the approval process once again. On occasion it is appropriate to request more than one domain name/host name per server. The number of host names is limited to **eight** per physical server or network address and each server may have no more than **one** network adaptor. If a network device is moved to a different subnet, its domain name must be re-registered with IRM and a new network address assigned. IRM naming conventions must be followed wherever possible and appropriate. If any particular domain name/host name or network address creates a problem on the network, as is the case when duplicate names and/or addresses attempt to coexist on the same subnet, IRM will notify the owner and issue a new name.

#### G. 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. If other wireless devices in use cause interference with the FAU network, IRM will work with the college, department or administrative unit owning the device to find an alternative solution.

Wireless network traffic will be confined to its own VLAN where network authentication is mandatory. Users will be required to have an FAU account for authentication prior to accessing the wireless network. Wireless transmissions are not secure. All users should exercise caution in accessing sensitive or personal information while using the wireless network. For information on IRM supported hardware and software refer to <http://www.fau.edu/irm/wireless/>.

#### H. 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 FAU network found in non-compliance with these restrictions will be disconnected immediately.

#### I. Peer to Peer (P2P) File Sharing and Software Piracy

Florida Atlantic University does not permit the illegal downloading and/or sharing of copyrighted materials in any form or manner. If a member of the University community violates this policy the following penalties will be enforced:

*Enforcement Process:*

*Resident and Non-Resident Students*

*First Violation:* The student's internet access from their computer will be shut down briefly (24 hours) after a pop-up warning appears on the violator's computer screen. The pop-up warning will inform the student that he/she will have access to university applications in any Open IRM Computer Lab. The Housing office will be notified.

*Second Violation:* The student's Internet access from their computer will be shut down for 72 hours and/or the student completes a tutorial through the Division of Information Resource Management (IRM) regarding appropriate computer use. The Dean of Student Affairs office will be notified.

*Third and Subsequent Violations:* This matter will be referred to the Dean of Student Affairs office for further action pursuant to the Florida Administrative Code for Student Conduct. The student's internet access from their computer will be suspended until this matter is resolved.

Students who violate the policy and have their room access shut off could still go to university labs to do school work and check their email. IRM could also block the student's account from going outside of the University, in other words, suspend external access only.

*Enforcement Process:*

*Faculty, Staff and Administrative Personnel*

*First Violation:* Internet access from their computer will be shut down briefly (30 minutes) after a pop-up warning appears on the employee's computer screen.

*Second Violation:* The employee's supervisor will be notified. The supervisor must meet with the employee to counsel him/her. Any further action will be at the supervisor's discretion.

*Third and Subsequent Violations:* Notice will escalate to the next level supervisor for action. A record of the action may be placed in the employee's personnel file.

## J. 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.

## K. Electronic Mail (Email) and Spam

All email sent and received 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. If your email falls within the definition of a public record, you may not delete it except as provided for in the university's retention schedules. Non-compliance with this law will result in disciplinary action. For detailed information regarding retention of public records refer to the Florida General Records Schedule GS5 for Universities and Community Colleges found at <http://dliis.dos.state.fl.us/barm/genschedules/g505.pdf>. In compliance with this law, IRM makes nightly backups of all email on our mail server and will keep a copy of these email messages for three years.

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
- Attempts at sending viruses

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.
- Political messages.
- 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.

IRM does not condone the practice of spamming, i.e. sending spam as identified above. To reduce the risk of receiving spam or email messages used to deliver computer viruses, IRM is considering a system, for university mail servers that requires other mail servers sending mail to FAU users have reverse DNS lookup enabled. If the communicating server does not have this featured enabled mail messages will not be accepted from that server. 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. (Refer to Policy VI, Acceptable Use and Ownership of Technology Resources.) Each user account is assigned specific resources for use by email messages. It is the user's responsibility to stay within these resource boundaries. Authorized users are responsible for ensuring that their email is downloaded to their desktop computers and systematically deleted from the FAU server on a timely basis. IRM reserves the right to delete email when it exceeds the limits of said resources. Furthermore the size of email messages and attachments is limited to 10 MB. Messages exceeding these limits rapidly consume system and user resources interfering with the delivery of all email. As a result messages and/or attachments greater than the allocated size will be refused by the mail system.

IRM encourages the use of electronic mail; however, users shall have no expectations of privacy. IRM may access any and all electronic mail at any time in accordance with Section V. D. of this Information Resource Management Policy. 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 various purposes, including but not limited to:

- troubleshooting hardware and software problems

- preventing unauthorized access and system misuse
- rerouting or disposing of undeliverable mail
- Approved monitoring situations , as defined in Section V.D. of this Information Resource Management Policy.

IRM will need the approval of the Associate Provost of IRM or his/her 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.

## L. Email Accounts

### *Faculty and Staff*

IRM provides email accounts to all university administrators, faculty, adjunct faculty and staff during active employment. Effective January 2005, biweekly pay stubs are emailed to the FAU email address of all FAU employees who have direct deposit. Additionally, it is requested by the FAU administration that all work related electronic communication use a valid FAU email address. After employment is terminated, the account will be disabled immediately and physically removed from the system after 60 days. The sole exception to this rule is retired faculty accounts. All existing accounts for employed personnel are verified annually. Adjunct faculty accounts are disabled annually at the end of the Summer semester. Renewal of adjunct faculty accounts must be initiated by the sponsoring department prior to the Fall term. Attachments are limited to 5 MB.

**Email accounts are provided for all students from the point of application to the University. All official FAU communication to students will use the student's FAU email account. One year after graduation or after three successive semesters during which a student has not been registered for a course, the account will be disabled. All student e-mail accounts will be verified each semester. Students may forward e-mail from their FAU account to another e-mail address of their choice but it is not recommended. Email attachments are limited to 8 MB.**

### *Special Request Email Accounts*

Other types of accounts issued by IRM include general departmental email accounts, courtesy accounts for specially authorized friends of the University and temporary accounts. Departmental and courtesy accounts are verified annually. Temporary accounts are intended for visitors who require network access for a short period of time. They have built-in expiration dates and are evaluated weekly. All expired temporary accounts are deleted without backup.

Departmental, courtesy and temporary e-mail account requests must come from

the department head or designated representative and include the name of the account sponsor, the start and end date for the account and an account justification. The conventions for account names are:

- Faculty, staff, and student accounts are created with the first initial of the first name and up to seven letters of the last name. Faculty and staff may choose to have an alias of `firstname.lastname@fau.edu` .
- Temporary accounts are created using the identifier assigned to the request, for the account, by the IRM Help Desk. For multiple accounts requested concurrently the identifier will be followed by a letter of the alphabet.

#### M. Distribution Lists

Groups within MyFAU will be created in the place of distribution lists. MyFAU groups provide email service to all group members. Complete and submit group requests through the Groups application within MyFAU.

#### N. World Wide Web

IRM supports the FAU.EDU web domain to provide web access to FAU services and information. IRM makes available the use of FAU.EDU to colleges, departments, campuses and other FAU organizations to further support the mission of the University. Users of FAU web servers are responsible for the content and information they store on these systems and are expected to abide by IRM technology policies as defined here. Any person wishing to become a web developer on the FAU.EDU domain must already have an FAU email account. The Web developer account will allow access to the Web server for the creation of new departmental pages and the maintenance of existing pages. All FAU web developers are given 10MB of disk space initially. IRM will increase disk space for legitimate reasons only.

Web pages created by university-related organizations must be consistent with policies set by University Communications and Marketing. Personal web pages should clearly indicate that the pages reflect the owner's opinions and not those of the University.

#### O. Commercial Web Use

Using the FAU Wise Web server system for commercial purposes is not permitted.

#### P. WISE Privacy Policy

IRM collects no personal information about visitors to the FAU website unless it

is the desire of the visitor to make such information available. IRM gathers information regarding the volume of access to the website at any given time by collecting information on the date, time and web pages accessed. IRM's intent is to improve the content of our website. Visitors to the FAU website are encouraged to read the privacy policy posted there, [http://www.fau.edu/notices/privacy\\_policy.html](http://www.fau.edu/notices/privacy_policy.html).

## VII. 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 FAUNetID. 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.***

Open student computing labs are for use by faculty, staff and currently registered students only. The Broward computing labs will accommodate faculty, staff and students from FAU, Florida International University and Broward Community College. Instructional labs are used for teaching purposes only, except in the case of dual purpose labs which are used as both teaching and open computing labs. Students who wish to continue using an instructional lab at the conclusion of a class may only do so with the permission of the Lab Manager or Lab Assistant, otherwise they must move to an open lab to continue working. Charges for lab use are applicable for non-curriculum based activities, student sponsored events, where an admission charge or fee is collected, and funded grant activities. More information on student lab usage and operations can be found in the IRM Computer Lab Guide Book, <http://pdp.fau.edu/documentation/labguidebook.pdf> .

### A. Student Computer Labs – Software

- All software installations not expressly permitted in writing by the Lab Manager is forbidden on IRM computing resources.
- All software installation requests on IRM computer servers or workstations must come from the professor/instructor responsible for the class requiring the software. The software must have an academic purpose or use and must be licensed for the use being requested. Requests from students or teaching assistants will not be considered. Unlicensed, illegal or incompatible software will not be installed for any reason. Software that duplicates the function of an existing software application will not be installed.

- All software installation requests must be made by way of the FAULABS Software Request Form found at <http://www.fau.edu/helpdesk/> and must be made in accordance with the FAULABS software installation request procedures.
- All software installation requests must be made 30 days prior to the first day of class.
- All software installed in a lab, per installation request procedures, must be tested by the professor/instructor, in the computer lab where the software will be used, 5 days prior to the first day of class. Any problems with the software must be reported via the FAULABS problem report form that is found on the desktop of every computer in every student computer lab.

## B. Instructional Computer Labs – Scheduling

### *Boca Raton campus*

- All scheduling requests must come from the professor responsible for the class to be held. Requests from students or teaching assistants will not be considered.
- All scheduling requests must be made directly to the Instructional Facilities Scheduler located in the Registrar's Office.
- Once an instructional lab has been reserved for use the professor and/or teaching assistant must notify the IRM Lab Operations Manager.
- The Lab Operations Manager will provide copies of the following procedures: *Lab Security and Card Access Procedures, Software Installation Procedures, Problem Report Procedures*. Each professor and/or teaching assistant must sign a statement saying that they have received, read, fully understand and agree to abide by this documentation. Receipt of this statement by Academic Computing Services is mandatory before card access to the instructional lab is given.

### *Broward campuses*

Reservations for instructional labs will be accepted from faculty only. Students and teaching assistants are not permitted to reserve instructional labs. Lab reservations should be submitted along with your initial course-offering request. Requests made after the course schedule has been released must be submitted directly to the Lab Manager and will be filled on a first-come, first-served basis. Reservation requests can be submitted to the Lab Manager online, at <http://www.bcs.fau.edu/forms/LabForm.html> .

## C. 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. For more information go to <http://www.fau.edu/housing/connect.html>

## **VIII. Peer Campus Computing Support**

FAU is committed to providing equal access to, and support of, information technology resources at each campus. Remote electronic access to all centralized services at the Boca campus is an integral part of support for peer campuses and will continue to be expanded in the future.

Computing policies on all campuses will be formulated based on FAU's computing policies developed by the Associate Provost of IRM. Further definition of these policies may be made to accommodate the unique programs of each campus. Requests for approval of such variations will be made to the Associate Provost of IRM or his appointee.

## **IX. Emergency Preparedness and Disaster Recovery**

### A. Emergency Use of the FAU Mail System

It is the policy of FAU to notify and protect its faculty, staff, students and visitors in times of impending natural and/or man-made disasters. The most efficient and effective means of doing so is via e-mail and the Internet, using the FAU Emergency Homepage.

Upon notification that a possible disaster condition exists, and once the Emergency Operations Committee (EOC), chaired by the President of FAU, decides that the University will close, all non-essential e-mail will be put on hold. Should it be determined by the EOC that FAU *will not be affected* by the possible disaster condition all e-mail distribution will continue as usual. Should it be determined by the EOC that FAU *will be affected* by a natural or man-made disaster an emergency e-mail distribution process will take effect immediately. The following sequence of steps will be carried out.

1. All e-mail currently set for distribution or in the process of distribution will be suspended and put into a holding queue for later distribution.
2. The emergency e-mail distribution protocol will immediately be activated by IRM. This protocol stipulates who is eligible to send e-mail through the FAU e-mail system in times of emergency.
3. Only e-mail identified as coming from the Office of the President and/or his/her designee will be accepted by IRM for distribution.

4. IRM will follow the procedures associated with this policy to ensure timely distribution of authorized e-mail during the emergency situation.
5. Upon the resumption of normal operations, IRM will proceed with normal e-mail distribution protocols and all e-mail held in the queue will be distributed.
6. If the FAU Data Center is inoperable, IRM will activate its disaster recovery site and will provide the EOC, or its designee, with a list of individuals authorized to send e-mail messages.

#### B. Emergency Changes to Voice Greetings And Web Pages

Emergency situations necessitate changes to voice greetings and web pages with current information for the general public regarding the University's status, special events, class schedule changes and any other relevant information. The University President and/or his designee must approve all such changes. IRM staff working in conjunction with the requesting departments, colleges or administrative staff will carry out the changes. (Refer to Provost Memorandum, "Emergency Change to Campus-wide Voice Greeting and/or Emergency Changes to the FAU WWW Homepage".)

#### C. FAU Emergency Policy

In the event of a disaster, IRM will follow the guidelines stated in the FAU Emergency Policy, <http://www.fau.edu/library/fauhurr.htm>. For additional information concerning the hurricane threat to the South Florida area in general and Florida Atlantic University in specific refer to <http://www.fau.edu/library/hurric.htm>.

#### D. Equipment

The following steps should be taken to protect all electronic equipment when threatened by a natural disaster.

- Phones are not to be unplugged. They should be placed in a desk drawer, cabinet or a plastic bag.
- Desktop computers and printers should be turned off, unplugged and wrapped in plastic.
- Servers should be turned off, unplugged and wrapped in plastic.

#### E. Backups

If the threat of a natural disaster becomes likely, backups of all essential computing systems by the responsible system administrators or their subordinates will commence immediately. At least one set of backups will be

stored off site at a predetermined location as established within backup procedures. IRM recommends that all university personnel back up all essential personal computer or workstation files to a removable media on a regular basis as a part of their departmental and/or college disaster preparedness plans.

#### F. Student Computer Lab Operations

If the threat of a natural disaster becomes likely during normal business hours and the President has not closed the University, all open computing labs and non-essential instructional labs will be closed at 2:00 pm to allow adequate time to initiate disaster preparedness procedures.

#### G. IRM Disaster Recovery Plan

IRM has developed a Disaster Recovery Plan in the event of potential or actual prolonged equipment failure or other situation that hinders access to or use of IRM computing resources. This plan will be put into effect by the order of the Associate Provost when conditions warrant. In addition to containing a checklist of actions to be taken, responsible individuals within IRM, contact information and maps, the following key areas are addressed.

- A. Hurricane/Floods
  - 1. General Information
  - 2. Storm Monitoring
  - 3. Hurricane Watch Procedures
- B. Fire
  - 1. Fire Prevention
  - 2. Fire Prevention Classes and Practice Fire Drills
  - 3. Emergency Action and Evacuation
- C. Civil Disorders and Vandalism
  - 1. Emergency Action Plan
  - 2. Advance Notice Action Plan
  - 3. Emergency Action and Evaluation
- D. Power Failure/Air Conditioner Failure
  - 1. Power Failure
  - 2. Brown Out
  - 3. Air Conditioning Failure
- E. Recovery
  - 1. Disaster Recovery Coordinator
  - 2. Evaluation Team
  - 3. Systems, Networking and Operations Teams
  - 4. Assistant Directors
- F. Establishing the Computer Center at a Backup Facility
  - 1. Backup Site
  - 2. Personnel Notification
  - 3. Facility Setup and Equipping

4. Software Restore Procedure
5. Remote Data Transmission
6. Equipment Availability
7. Personnel

## **X. Instructional Technology Support and Distributed Learning**

IRM is responsible for university-wide distance learning functions. Faculty members are responsible for program coherence, course content and appropriate pedagogy. Recent advances in information technology have significantly expanded the range of course delivery modes from videotapes to interactive web-based learning tools. Each delivery mode, its associated policies and areas of responsibility are defined separately.

### A. Distance Learning

Blackboard is the IRM supported web-base distance learning platform at FAU. Faculty must complete the course space request form, to obtain course space in Blackboard, [http://www.fau.edu/irm/blackboard/bb\\_requests.php](http://www.fau.edu/irm/blackboard/bb_requests.php). Students will, automatically, be enrolled in web-only and web-assisted courses every day during the drop/add period at the beginning of each semester. Enrollments will be updated twice weekly after drop/add.

Faculty are required to attend Blackboard training either in formal classroom training sessions or in one-on-one sessions with an Instructional Designer before using BlackBoard for the first time. IRM recommends faculty work with ITSS to convert their traditional courses to an electronic format. Resources will be made available as well as the expertise of instructional designers to assist in the design and implementation of on-line courses or programs. Faculty should not be using commercial web sites with advertisements appearing on their course pages.

After faculty training and course development is complete, faculty should upload all of their course material themselves. ITSS **will not** upload course content to Blackboard for faculty. The purpose of the Blackboard hands-on training workshops (or one-on-one training) is to teach faculty to do manage their online courses independently.

It is the responsibility of each faculty member to backup their courses each time changes are made to the content. Blackboard courses remain on the server for one semester after they have completed. For example, during the spring semester all courses taught during the fall semester will still be available. At the end of each semester all of the previous semester's courses and grade books are backed up individually and then removed from the Blackboard server.

## B. Instructional Design and Development

The Instructional Design and Development group is responsible for assisting faculty and academic units with the design of on-line courses, programs and academic activities on all FAU campuses. Consulting services are available to evaluate course goals, objectives and outcomes together with prescribing instructional design and development strategies. Training workshops and seminars are also conducted to provide the skills necessary for faculty and staff to independently design on-line courses.

## C. Television and Video Production Services

IRM maintains staff and facilities to plan, schedule, produce, and distribute professional quality television, video, audio, and distance education products. Florida Atlantic University has six production facilities located on the Boca Raton campus. Complete electronic field production, editing and post-production services are available. Scheduling of all production activities, assignment of teleclassrooms and production personnel, and remote operations are handled by IRM's Department of Learning Resources, Television and Video Production Services. Fees are applicable to all activities except for credit distance education courses.

All visually recognizable individuals participating in video production must complete and sign a talent release form. This includes faculty, staff, students and guests included in the production. The execution of this form permits the individual to be videotaped, recorded, photographed or digitally recorded and permits future use or duplication of any media produced. A copy of the talent release form is available from the administrative offices of University Learning Resources. All signed and completed copies are kept on file.

## D. Television Engineering

IRM TV engineering staff design, operate and maintain broadcast radio frequency, microwave and closed circuit signal distribution systems, video production facilities, studios, and teleclassrooms. Other responsibilities include the development of specifications for multimedia presentation systems within auditoriums and/or classrooms, the maintenance of satellite downlink dishes and uplink equipment, visual arts installations, FCC licenses held by FAU academic or administrative units and the operation of an audiovisual repair facility. Any university owned audiovisual equipment may be sent to this facility for diagnosis and repair. The cost of parts necessary for repair will be charged back to the responsible individual, administrative department or academic unit. There will be no charge for labor. All equipment requiring maintenance or repair must be delivered to TV Engineering in University Learning Resources.

## **XI. Miscellaneous Issues**

### A. Health Insurance Portability and Accountability Act of 1996

FAU must comply with Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), <http://aspe.hhs.gov/admsimp/pl104191.htm>. Failure to comply with any aspect of this law will result in disciplinary and/or legal action.

### B. Grant Recovery for Computing Services

Sponsored research activities that require computing resources as provided by IRM must be in compliance with the Grant Recovery for Computing Services policy as defined by the Office of the President in Policy Memorandum #82.

## References

“Virtual Legality, An Overview of Your Rights and Responsibilities in Cyberspace”, Steven J. McDonald, Associate Legal Counsel, The Ohio State University, <http://legal.ohio-state.edu/virtual.html>

EDUCAUSE, Policy Initiatives, <http://www.educause.edu/policy/policy.html>

The Center for Democracy and Technology, <http://www.cdt.org/>

The Ohio State University IT Policies and Guidelines, <http://www.cio.ohio-state.edu/policies/>

The University of Florida Policies and Procedures: A List of Links, <http://www.admin.ufl.edu/division/vp/otherpp.htm>

The University of South Florida Health Services Center, Information Services Policies, <http://hsc.usf.edu/is/policies/index.html>

The University of Central Florida, Distributed Learning: Scope and Policies, [http://www.distrib.ucf.edu/dlucf/dlp\\_plain.htm](http://www.distrib.ucf.edu/dlucf/dlp_plain.htm)

Florida State University Policies and Responsibilities for Use of Campus Computer and Network Resources, <http://www.acns.fsu.edu/docs/policy.html>

Kansas State University, Computing & Network Services, Policies and Procedures, <http://www.ksu.edu/cns/policy/policy.html>

Mankato State University Student Computer Usage Policy for ACTS Resources, <http://www.mnsu.edu/dept/acts/web/acts.html>

Florida International University, Academic Affairs Policies and Procedures Manual, Section 11 – Academic and Research Computing, <http://www.fiu.edu/~arc/sec11.htm>

George Mason University, University Administrative Policy Number 60, Responsible Use of Computing Policy, <http://www.gmu.edu/mlfacstaff/findex.html>

San Diego State University Computing Security Policy, [http://www-tns.sdsu.edu/security/security\\_policy.html](http://www-tns.sdsu.edu/security/security_policy.html)

University of Wisconsin System, Financial and Administrative Policies, Information Technology, <http://www.uwsa.edu/fadmin/infotech.htm>

University of Houston, Information Technology, Policy and Reference Guide, <http://www.uh.edu/infotech/policies.html>

Health Care Financing Administration, The Health Insurance Portability and  
Accountability Act of 1996 (HIPAA) Page,  
<http://www.hcfa.gov/hipaa/hipaahm.htm>

Proposed Standards for Privacy of Individually Identifiable Health Information,  
<http://aspe.hhs.gov/admsimp/nprm/pvcsumm.htm>

Rev date: February 6, 2007

# Index

## A

Administrative Data Systems, 8  
Audiovisual equipment  
    Appropriate use, 12  
    *Repair*, 17  
    Requests for, 31

## B

Banner, 9  
Blackberry, 19

## C

Cable, 8  
Calling cards, 19  
Cellular phones, 19  
Computer Abuse Amendments Act of 1994, 3  
Computer Crimes Act, 3, 14  
Computer Fraud and Abuse Act of 1986, 3

## D

Desktop standards  
    Supported hardware and software, 11  
Digital Millennium Copyright Act, 3, 14  
Disaster recovery  
    Backups, 32  
    Equipment, 13, 15, 16, 17, 18, 32, 34  
    FAU Emergency Policy, 32  
    IRM Disaster Recovery Plan, 33  
Distributed Learning, 37  
    Blackboard, 34  
    Consulting Services, 35  
Dynamic Host Configuration Protocol (DHCP), 22

## E

Email  
    Accounts, 15, 27  
    Emergency use of, 31  
    Privacy, 28, 38  
    Public record, 25  
    Retention of, 25  
    Spam, 25

## F

FAUNetID, 9, 15  
Firewalls, 25  
FTP, 24  
    Anonymous FTP, 24

## H

HIPAA, 36, 38

## I

IRM supported software  
    Access to Computers, 10  
    Banner, 9  
    MyFAU, 9  
    SSL, 11  
    Web pages, 28

## M

Multimedia, 15  
    Appropriate use, 12  
    Requests for, 31  
    TV Engineering, 35

## N

Network  
    Bandwidth, 20  
    Cable, 8  
    DHCP, 22  
    Firewalls, 25  
    Hacking, 21  
    Network address, 22  
    Port scanning, 21  
    Sniffing, 21  
    Telecommunications equipment, 17  
    Videoconferencing, 16, 17  
    Wireless, 23, 24

## O

Obscenity  
    Email, 25, 27

## P

Peer to peer file sharing, 24  
    Software piracy, 24  
Public Records Law, 3, 25

## S

Secured Socket Layer, 11  
**Software**  
    Firewalls, 25  
    Hacking, 21  
    Installation, 18, 21, 30  
    Intellectual Property Rights, 15  
    Peer to peer file sharing, 14  
    Piracy, 24  
    Problems, 18  
    Purchasing, 11  
    Supported, 8  
    Training, 35  
    Training, 11  
Student computing

Instructional lab, 29  
**Privileges**, 29  
Wireless, 23, 24

## T

### Technology resources

Audiovisual, 15  
Multimedia, 15  
Ownership and use of, 26  
**Software**, 8, 11, 13, 29, 30, 34  
Telecommunications, 17, 18  
Unauthorized use, 16  
Videoconferencing, 16, 17  
Telecommunications, 17, 18  
Activation costs, 18  
Calling cards, 19  
Equipment, 13, 15, 16, 17, 18, 32, 34  
Resources, 8, 12, 14, 16, 35, 37  
Trouble line, 18  
Teleconferencing  
Facilities, 8, 30  
Installation, 18, 21, 30  
Services, 8, 11, 17, 18, 19, 30, 35, 36, 37  
Television  
Engineering, 35  
FCC licenses, 35

Videoconferencing, 16, 17  
Training, 11, 35  
Blackboard, 34

## U

University Databases, 8  
User accounts  
Privacy, 28, 38

## V

Videoconferencing, 16, 17  
Administrative VC Network, 16  
Overview, 37  
Rooms, 13  
Standards, 38  
Visual communications  
Resources, 35, 37

## W

Wireless, 23, 24  
WISE server, 15  
World Wide Web, 15, 28  
Commercial use, 28