Facilities Information Technology Policy & Usage Guidelines

OBJECTIVE

This policy statement is intended to support appropriate and effective use of information technology (IT) resources at the Facilities Department of Florida State University (FSU), while providing guidelines for allowable use.

OVERVIEW

- Facilities provide a wide variety of IT resources, including computers, networks, software, computer accounts, hand-held and wireless devices, for use by Facilities' staff. These resources are administered by the Facilities Information Technology department, and they are intended for the legitimate business of the University.
- Appropriate business use of IT resources includes instruction, research, and the official work of the offices, departments, and other agencies of Facilities. Priority for resources may be granted to certain users or certain groups of users in support of the Facilities' mission.
- Computer accounts are provided to staff as a privilege associated with membership in the Facilities community. When an individual accepts this privilege, a number of responsibilities must be assumed, including knowledge of appropriate Facilities and University policies and procedures.
- In recognition of the World Wide Web (WWW) as an important communication medium, Facilities encourages its use as a means of supporting and fulfilling the mission and official work of the University.
- It is critical that technology systems maintain adequate security and we safeguard the confidentiality of data.

REQUIREMENTS AND PROHIBITED USES

- All uses of Facilities IT resources are subject to applicable rules, policies and procedures of the University and/or governing boards as well as Florida Statutes governing computer fraud, misuse of state equipment resources, public information, and related criminal offenses.
- Any commercial use of Facilities IT resources by an individual must be pre-approved consistent with existing University policies and procedures regarding outside employment.
- Commercial advertising on unofficial Web sites using a Facilities computing account is a violation of University policy. Individuals are prohibited from using their computing accounts in association with any personal commercial purpose or enterprise.

- Occasional, incidental personal use of IT resources is permitted by this policy, except when such use:

    a) Interferes with the performance of the user's job, employment or other Facilities responsibility.

    b) Results in additional incremental cost or burden to the Facilities IT resources.

    c) Is otherwise in violation of this policy.

- This does not preclude additional limits on personal use of Facilities equipment as may be determined by individual units within the Facilities Department in accordance with normal supervisory procedures.

- Owners of computer accounts are responsible for all use of the accounts. They should prevent unauthorized use by others and report intrusions to the Facilities IT department. Under no circumstances should any employee use any computer account other than one assigned to them by Facilities IT when operating on Facilities computers. Anyone found violating this guideline may be subject to disciplinary action.

- To help maintain the proper functioning of computer and networking hardware and software, Facilities will take reasonable steps to ensure its computing resources are free of deliberately destructive software, such as viruses. Individuals must share responsibility for protecting Facilities computers and should ensure the integrity of any electronic media they introduce.

- Respect for intellectual labor, creativity, and the right to privacy is vital to our enterprise. System integrity is also essential for individual function. Invasion of privacy and unauthorized access to files can be justified only by real threats to the integrity of the network or node.

- Owners of computer accounts are not allowed to install/remove software, make critical system changes, or otherwise deface or impede the normal operations of IT resources without prior authorization from the Facilities IT department

- Purchases of IT related resources including but not limited to software, monitors, printers, networking equipment, etc are to be approved and purchased by the Facilities IT department.

- No unauthorized equipment will be plugged into the Facilities network. This includes home laptops, gaming devices, personal monitors, keyboard and mice, USB thumb drives are acceptable.

- Facilities IT department offers support to FSU purchased equipment/applications only. User's personal equipment will not be supported or maintained by the IT department in any capacity.

- Users experiencing any IT related problems are to contact the Service Center to request help. Please be ready to provide the following information to the Service Center agent when you call:

    a) User's Name

    b) Machine Host name or equipment type

    c) The exact nature of the problem including but not limited to error messages, noises, actions performed by the user before AND after the problem occurred, etc.

    d) An honest assessment of the urgency of the request.

- The creation of new user accounts is to be handled through the Facilities IT Department via a Work Order submitted by the Service Center. Account requests are to be handled by the supervisor of the individual needing access. Please be prepared to provide the following information:

    a) Employee name

    b) Employee section

    c) Access required (i.e. Domain account, email, AiM, etc)

- Requests for new online forms, reports, documents and other electronic media are to be submitted via work request to the Facilities IT Department for review and publication to the web or elsewhere. Please include as much detail as possible when submitting requests. In most cases, a meeting will be held to determine the exact specifications of the request.

- The official FSU IT Policies & Guidelines should be reviewed for further descriptions of requirements. The official policies can be found at http://www.vpfa.fsu.edu/policies/bmanual/itpolicy.html

B. ELECTRONIC MAIL AND ELECTRONIC COMMUNICATIONS

- Facilities supports open access to electronic communication and information and members of Facilities may freely communicate and access information on electronic networks, provided that the following guidelines are observed:

- Material accessible to the Facilities community through networks and materials disseminated from the University should not be restricted on the basis of content, nor because of the origin, background, or views of those contributing to its creation. However, University IT resources may not be utilized:

a) For personal financial or commercial purposes.

b) To access or view pornographic or obscene materials.

c) To impersonate another person or misrepresent authorization to act on behalf of others.

d) To state or imply, without authorization, that a user speaks or acts on behalf of the University.

e) To harass another person. Users should not transmit to others or display images, sounds, or messages that might be perceived by a reasonable person as being, or have been identified as, harassing.

f) To invade the privacy of others or make unauthorized use of their work. Users should not attempt to read or copy files belonging to others, or decrypt or translate encrypted material, unless the files have deliberately been made accessible by the owner(s) or authorization has been obtained to do so.

g) To send or create junk mail, spam, chain letters, computer viruses or hoaxes, or other disruptive material.

h) To intentionally damage or disable computer systems, networks, or software.

i) In violation of federal, state, or local law governing use of computer and information technology. Unauthorized or fraudulent use of the University's computing resources may result in felony prosecution and punishment as provided for by state or federal law.

j) In violation of copyright laws.

k) In violation of University or governing board rules and regulations concerning computer and information technology.

l) To undermine the security or the integrity of computing systems or networks or to attempt to gain unauthorized access. Users may not use any computer program or device to intercept or decode passwords or similar access control information. Security gaps should be reported to the appropriate system administrators.

m) To copy or use software, except as explicitly permitted under licensing agreements. Computer users should be able to prove ownership of software in their possession.

n) To delete or destroy public records without authorization.

o) Public records. Any information, including e-mail messages or other data, produced, transmitted, or received by University employees "pursuant to law or ordinance or in connection with the transaction of official business" is defined as a public record by Florida Law, and is subject to the provisions of Chapter 119, Florida Statutes. Public records must be retained according to specific retention schedules, are subject to inspection and copying upon request by any member of the public (except as specifically exempted by law), and may not be deleted or destroyed except as authorized by law. Responsibility for adhering to public records requirements is the individual responsibility of each employee. Subject to public records law(s), Facilities supports each individual's right to private communication, and will take reasonable steps to ensure security of the network; however, Facilities cannot guarantee absolute privacy of electronic communication.

p) Electronic forums such as mail distribution lists and Usenet newsgroups all have expectations regarding subject area and appropriate etiquette for postings. Members of the Facilities community should be considerate of the expectations and sensitivities of others on the network when posting material for electronic distribution to group listings. These group email listings will be used only for work related correspondence.

C. PRIVACY AND SECURITY

- Facilities cannot guarantee that, in all instances, copies of critical data will be retained on FSU systems. Our DRP states that we provide a 24mth retention period for data files.

a) All work related documents are to be stored in the appropriate departmental folder on the shared directory, mapped to the S:\drive. This folder will point to a shared directory on the NAS for secured storage and backup purposes.

b) Any personal documents are to be stored on the user's B:\drive. Work related audio, video and image files should be stored on the shared drive (s:\drive). Audio & video files are not permitted on users profiles. Audio files found on users personal b:\drive's will be deleted immediately and

followed by an email notification to their supervisor advising of the policy violation, which may result in disciplinary action.

c) Any non-work related image files are not to be stored on the network. Any non-work related image files will be deleted immediately and followed by an email notification to their supervisor advising of the policy violation, which may result in disciplinary action

d) The supervisor should work with the employee prior to termination date to move all work related data to the appropriate departmental folder on the shared drive.

e) Any account that has been inactive for a period of 30 days or more will be disabled. An email will be sent to the supervisor advising them of this change in account status. It is the responsibility of the supervisor to notify the Facilities IT department of any circumstance surrounding the employee in question that would require this account to remain active beyond this time frame.

f) All accounts inactive for 60 days or more, without notification of Facilities IT, will be deleted from the network.

D. VIOLATIONS AND ENFORCEMENT

- Users who violate these policies may be denied access to Facilities IT resources and may be subject to other penalties and disciplinary action, both within and outside the University. Violations may be handled through the University disciplinary procedures applicable to the relevant user. Additionally, Facilities may temporarily suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Facilities or other IT resources or to protect the University from liability. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.