University of Florida Foundation, Inc. (UFF)
Acceptable System Use

Policy #: 3.08
Effective Date: August 9, 2010
Responsible Department: Computing

1. PURPOSE

To protect UFF and ODAA and their employees, and the information stored in UFF's system, by ensuring the security of the computing system and outlining what constitutes acceptable uses. Inappropriate use exposes UFF to risks, including virus attacks, compromise of network systems and services, and legal issues.

2. APPLICABILITY

All computing systems and resources, including, but not limited to, data, computer equipment, software, operating systems, storage media, network accounts providing electronic mail and internet usage, are the property of UFF and must be used for the benefit of UFF and ODAA. **No employee shall have any expectation of privacy in any technology provided by UFF including equipment, such as laptops and PDAs, and services such as email and internet usage.** Use of any of these resources by any third party shall also be subject to these terms.

3. POLICY

Effective security is a team effort involving the participation and support of every UFF and ODAA employee.. Every user is responsible for knowing these guidelines and conducting his or her activities accordingly.

General Use and Ownership

1. Users should be aware that all data created on UFF systems is and remains the property of UFF. All data is confidential and should be handled accordingly.

2. Employees shall exercise good judgment regarding the reasonableness of personal use. Use of the internet is intended primarily for the conduct of UFF/ODAA business. Limited, occasional, or incidental use of internet access for personal non-business purposes is understandable. However, employees need to be responsible, and not allow personal internet usage to be detrimental to productivity.

3. Employees are strictly prohibited from accessing or displaying any materials that are sexual in nature, or that are otherwise offensive, derogatory, or illegal. Internet activity may be monitored by UFF or a record of it retrieved, if necessary.

Employees, by using UFF's computer systems, expressly consent to such monitoring.

4. For security and network maintenance purposes, authorized individuals within UFF may monitor equipment, systems, and network traffic at any time. It may be necessary on occasion for staff to enter an employee's office to maintain the computer. Permission will be obtained from the employee or a manager prior to entry.

5. UFF reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. It is the user's responsibility to understand and take appropriate precautions with respect to use and handling of sensitive and restricted data, in compliance with the Security Review and Data Classification Standard.

2. Employees must keep passwords secure and must not share accounts. Authorized users are responsible for the security of their passwords and accounts, and must comply with the Password Guidelines and Procedures for Users.

3. Work areas must be secured when unattended, in accordance with Workstation User Guidelines.

4. Because information contained on laptops is especially vulnerable, special care should be exercised. Laptops must be protected in accordance with the Mobile Computing/Laptop Guidelines and Remote Access Standards.

5. Any employee who uses a personal computer to connect to the UFF Web applications (Email, Advance, etc.) from work or home must have current virus application and updates. Permission to use the VPN and log into the corporate network requires approval and setup by Computing, as set forth in the Mobile Computing/Laptop Guidelines and Remote Access Standards.

6. Employees are required by law to report immediately any equipment or Restricted data that has been lost, stolen, or misplaced. (See Policy 1.06 Information Technology Security Policy and the Incident Reporting Procedures for Users.)

7. Employees who handle or have access to Sensitive or Restricted data are required to attend the Annual Security Review and Network Orientation. (See Policy 1.06).

8. Employees who send or transfer Restricted Data are required to encrypt the data. (See Guidelines for Transferring Restricted Data.)

9. Employees are required to review all User Standards and Procedures posted at **https://www.uff.ufl.edu/intranet**, Internal Business Units, Computer Services.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities *(e.g.,* systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

The list below is not exhaustive, but intended to provide a framework for activities which fall into the category of unacceptable use.

Under no circumstances is an employee of UFF or ODAA, or any other user of the UFF system, authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing UFF-owned resources.

The following activities are strictly prohibited:

1. Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property law, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UFF. This includes unauthorized copying of copyrighted material including digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which UFF or the end user does not have an active license.

2. Deliberately introducing malicious programs into the network or server. In addition, such actions as downloading anything from the internet (screen savers, toolbars, etc.), finding a USB memory stick and plugging it into a UFF computer, and other similar activities are prohibited.

3. Revealing an account password to others or allowing use of an employee's account by others, including family and other household members.

4. Using a UFF computing asset to actively engage in procuring or transmitting material that violates sexual harassment or hostile workplace laws or UFF policies.

5. Using a UFF email address to make fraudulent offers of products, items, or services.

6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these actions are within the scope of regular duties.

7. Any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job duties.

8. Circumventing user authentication or security of any computer, network, or account.

9. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's account, via any means.

10. Providing information about, or lists of, UFF employees, alumni, donors, or friends to unauthorized parties outside UFF.

11. Downloading software from the internet or loading personal software, including screen savers, toolbars, etc. (Refer to Web Navigation Guidelines, Email Guidelines for Users.)

Email and Communications Activities

The email system maintained by UFF is provided to assist in the conduct of UFF/ODAA business. Email system hardware and software are UFF property.

All messages composed, sent, or received on the system are UFF property. **No employee should have any expectations of privacy in any message**. Email communications to and from employees on the UFF system may be monitored by UFF and are subject to inspection by a supervisor or a member of management at any time as authorized by the Executive Vice President or the Associate Vice President. Employees, by using UFF's email system, expressly consent to UFF's monitoring of messages.

Limited, occasional, or incidental use of email for personal, non-business purposes is understandable. However, employees need to be professional and responsible and not abuse this privilege.

Certain uses are strictly prohibited, including the following:

1. Solicitation by email to any other email address with the intent to harass (spam) or to collect replies (conducting personal business).

2. Creating or forwarding "chain letters", "Ponzi" or pyramid schemes of any type.

3. Offensive, disruptive, improper, or unlawful messages, such as those containing sexual implications, racial or religious slurs, or gender-specific comments.

4. Messages that are defamatory, obscene, or otherwise inappropriate to the workplace.

5. Messages intended to annoy, harass, or intimidate another person.

6. Illegal purposes, such as gambling.

Employees shall not retrieve or read another employee's email mailbox without that employee's express written or electronic authorization, except as part of any monitoring activity authorized by the Executive Vice President or Associate Vice President.

Appropriate non-UFF related solicitations (*e.g*., sales of candy for school, sale of a piece of furniture) may be made to the "Bulletin Board" email group during non-work hours to avoid disrupting the work day (8-5). An employee may request to have his or her name removed from the Bulletin Board List by contacting the Computing Help Desk.

Access to another staff member's files, calendar, or contacts must be granted by that staff member in writing or by appropriate electronic designation. If the individual is not available, the request must be made by the individual's supervisor, in writing. The supervisor is responsible for notifying the user that access was granted to the user's information and why.

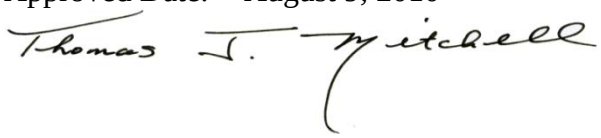
Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4. CLARIFICATION

Requests for clarification of this policy should be sent to the Interim Chief Technology Officer (cgrimes@uff.ufl.edu).

Approved Date: August 9, 2010



Thomas J. Mitchell, Executive Vice President

Revision history: Original version
Revised August 9, 2010
Reissued August 23, 2013