Acceptable Use Policy

Version: 6.0
Effective Date: 3/29/2016

Policy Summary:
An effective, robust, and secure information technology environment ("IT environment") is vital to The University of Tampa. To that end, the University provides an information technology environment which includes an array of institutional electronic business systems, computing services, networks, databases, and other resources (collectively, "UT IT resources"). These resources are intended to support the scholarship and work activities of members of the University's academic community and their external collaborators, to support the operations of the University, and to provide access to services of the University and other publicly available information. Access to and usage of UT IT resources entails certain expectations and responsibilities for both users and managers of the IT environment.

Questions about this policy should be directed to the VP, Information Technology and Security (813) 257-7522.

Applicability/Eligibility:
This policy applies to any individual, organization, group, entity, or third-party using University of Tampa computing or communications resources for voice, data, or video transmissions from on or off campus. It encompasses but is not limited to all University wired and wireless networks, academic and administrative systems, e-mail, Internet, University websites and social media, telecommunications, audio/video equipment, peripheral devices (printers, digital signage, cameras, etc.), faxed messages; University and personal computers, cellphones, and other mobile devices.

Exceptions:
None

Policy Administration:

Mandating Authority: (Check all that apply)

- ☐ Federal Law
- ☐ State Law or Regulation
- ☐ University President
- ☐ Accrediting Body
- ☐ Other: (specify)

Responsible Office/Dept/Committee(s):

Name	Campus Address	Phone Number
Information Technology & Security	East Walker Hall, Rm 133	813-257-7522

Responsible Executive(s):

Name	Title	Phone Number
Tammy L. Loper	VP, Information Technology and Security	813-257-7522

Policy Management:

Policy History:

Date	Version	Reason for Change
1/13/2004	1.0	Initial Policy
4/5/2004	2.0	Copyrights and Intellectual Property edit
4/5/2009	3.0	Expanded scope to include multimedia and mobile devices
1/9/2013	4.0	Added sections: *Security, Privacy, and Public Records, Social Media*, *Policy Amendments*. Clarified sections: *Brief Policy Summary (replaced Rationale or Purpose)*, *Applicability/Eligibility*, *Authorized Access, Protection of Assets and Information, Malware Prevention, Harassment, and Other Prohibited Activities*, and included the role of the Chief Information Security Officer
2/17/2015	5.0	Added: Protecting departmental accounts and requirement for student workers to use SE accounts to access files and folders on the campus network.
3/10/16	6.0	Incorporates organizational changes

Policy Approvals and Reviews:

Date	Organizational Group
3/29/16	President
3/29/16	Senior Staff
3/14/22	Changed last name of VP from Clark to Loper. No other changes

Web Links:

Policy Link: www.ut.edu/AUP

Full Policy Text:

Activities utilizing University computing and communications resources must be in accordance with University Policies, Faculty Handbook, Employee Handbook, Student Handbook, Student Code of Conduct, relevant local, state, federal, and international laws/regulations and the following guidelines:

Authorized Access

Users Should:

- Use University resources only for authorized purposes.

- In operating its IT environment, the University expects system users to engage in "safe computing" practices, such as establishing appropriate access restrictions for their accounts, setting strong passwords and guarding those passwords, keeping their personal operating systems and software applications up-to-date and patched, and employing security measures on personal devices used to store University information.
- Protect your campus user ID (or username), password and system from unauthorized use. Users are responsible for all activities associated with their user ID or that originate from their system and/or network wall jacks.
- Protect departmental accounts by restricting use to select staff for monitoring email accounts or accessing specific network files/folders. Departmental generic accounts are not intended to replace individual Spartan network domain accounts.
- Ensure that student employees use (SE) Spartan network domain accounts when their job duties include the need to access files and folders on the network, or to gain access to enterprise applications**.**
- Access only information that is your own, that is publicly available, or to which you have been given authorized access.
- Choose 'strong' passwords, protect them, and change them regularly.

Users Should Not*:*

- Attempt to decode passwords or access control information.
- Disseminate University information without proper authorization.
- Share staff or departmental accounts with student workers to circumvent the requirement for individual student employee (SE) Spartan network domain accounts.
- Use another person's system, user ID, password, files, or data without the written permission of the Chief Information Security Officer.
- Install an enterprise server (providing services to multiple people) unless the Office of Information Technology approves your request. Servers are only permitted if they do not contain critical/sensitive, regulated/operational data, are properly secured and registered with the Office of Information Technology, and any critical or high level security issues identified in vulnerability scans are promptly remediated.
- Use University systems or networks for personal gain, commercial, illegal, unethical, or partisan political purposes.
- Implement your own network infrastructure. This includes, but is not limited to basic network devices such as hubs, switches, routers, hardware firewalls, and wireless access points. Users must not offer alternate methods of access to UT resources such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS.

Protection of Assets and Information

Each user is responsible for the security and integrity of any system connected to the network, including the information stored on University computer systems.

Users Should:

- Make regular backups of information and files
- Secure sensitive and confidential information appropriately
- Control and secure physical and network access to electronic resources and data
- Properly log out of sessions

- Monitor access to their accounts (if a user suspects that their passwords or accounts have been compromised or that there has been unauthorized activity on their accounts, they are to report it to the **Chief Information Security Officer**, and change passwords immediately)

Users Should Not:

- Copy or store unencrypted sensitive or confidential information to insecure media such as system hard drives, removable hard drives, USB keys, smart phones, or other mobile devices
- Download programs containing malware that can damage the integrity of the systems and information they use
- Provide access to or information about their accounts or passwords to individuals over the phone, through emails, or in person unless they verify the validity of the request
- Attempt to circumvent or subvert system or network security measures

Malware Prevention

Campus Network users are responsible for transmissions originating from their computer systems and/or network wall jacks. A system infected with malware and/or remote control software (Bots) may be taken off the network without notice if necessary until the system is reinstalled and/or the problem is remediated successfully.

Users Should:

- Have current computer/mobile device protection programs (malware prevention, firewalls, etc.) and current operating system updates installed on their computer prior to connecting to the network.

Users Should Not:

- Engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating malware, disrupting services, damaging files or making unauthorized modifications to University data.

Security, Privacy, and Public Records

The University employs various measures to protect the security of its IT resources and user accounts. However the university cannot guarantee complete security and confidentiality. It is the responsibility of users to practice "safe computing" by safeguarding their passwords, changing them regularly, and protecting the information they process, store, or transmit.

Users should also be aware that their use of University Information Technology & Security resources is not private. While the University does not routinely monitor individual usage of its ITS resources, the normal operation and maintenance of the University's ITS resources require the backup and caching of data and communications, the logging of activity, monitoring of general usage patterns and other activities necessary or convenient for the provision of service.

The University may monitor University of Tampa resources and retrieve communications and other records of specific users of UT resources, including individual login sessions and the content of individual communications, without notice.

While every effort is made to insure the privacy of University of Tampa electronic records, employees are granted use of electronic information systems and network services to conduct University business, there may be instances when the University is obligated to produce information stored on the University network and/or computers.

Social Media

UT recognizes that social media sites can be effective tools for exchanging information and raising the visibility of the University. Therefore, employees may contribute content about UT and their work. However, employees are required to follow the **Social Media Policy** when maintaining a university-sponsored site. The University will take action in accordance with the Acceptable Use Policy if the Social Media Policy is violated.

Excessive Usage

Users Should:

- Be considerate in your use of shared resources.

Users Should Not:

- Users should not monopolize systems, initiate bandwidth intensive programs, overload networks with excessive data, send chain letters or unsolicited mass mailings, or utilize excessive connect time, disk space, printer paper, or other resources.

Copyrights and Intellectual Property

Users Should:

- Use only legal versions of copyrighted materials including software in compliance with vendor license requirements.

Users Should Not:

- Copy, use, or share copyrighted digital information files, including but not limited to articles, books, music and movies without legal authorization.
- Store such copies on University systems, transmit or share them over University networks.

Harassment

Users Should:

- Respect individuals' rights to be free of intimidation, harassment, and offensive behavior.

Users Should Not:

- Participate in a pattern of conduct that interferes with performing one's assigned role.
- Use e-mail or messaging services to harass or intimidate another person.
- Send email chain letters or mass mailings for purposes other than official University business.

Spoofing/Fraud

Users Should:

- Be on the alert for phishing attempts to gain access to private/protected information.

- Only share University information as appropriate with authorized individuals/companies/agencies.

Users Should Not:

- Use University systems or network as a vehicle to gain unauthorized access to other systems.
- For purposes of deception, transmit any electronic communications using a name or address of someone other than the assigned computer or account user name or address.

Reporting Suspected Acceptable Use Policy Violations

Anyone who has reason to suspect a deliberate or significant breach of the University Acceptable Use Policy should promptly report it to the UT Chief Information Officer.

Enforcement/Consequences

Violators may have their electronic access revoked and may be subject to disciplinary action as prescribed in University Policies, the Student Handbook, and the Employee Handbook. Offenders also may be prosecuted under laws including (but not limited to) the Communications Act of 1934 (amended), the Family Educational Rights and Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, Digital Millennium Copyright Act of 1998, and the Electronic Communications Privacy Act.

Information Disclaimer

The University of Tampa disclaims any responsibility and/or warranties for information and materials residing on non-University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of The University of Tampa, its faculty, staff, or students.

Policy Amendments

The university reserves the right to change the policies, information, requirements and procedures, announced in this policy, at any time. Changes required by University contractual commitments shall be effective and binding to users upon execution of any such contract by the University. A user shall be deemed to have accepted and be bound by any change in University policies, information, requirements, or procedures if such user utilizes E-resources at any time following announcement or publication of such change.