Acceptable Use Policy

Version 7.0

Effective Date: February 1, 2024

Policy Summary:

An effective, robust, and secure information technology environment is vital to The University of Tampa. To that end, the University provides an array of institutional electronic business and academic systems, computing services, networks, databases, and other 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 technology resources entail certain expectations and responsibilities.

Questions about this policy should be directed to the Vice President, Information Technology and Security (utcio@ut.edu).

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, email, Internet, intranet, University websites and social media, telecommunications, audiovisual 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
- ☒ University President
- ☐ Other: (specify)
- ☐ State Law or Regulation
- ☐ Accrediting Body

Responsible Office/Dept/Committee(s):

Name	Campus Address	Email Address
Information Technology & Security	TECH Building Room 383	utcio@ut.edu

Responsible Executive(s):

Name	Title	Phone Number
Tammy Loper	Vice President, 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: Se*curity, 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.
3/10/2016	6.0	Incorporates organizational changes
1/30/2024	7.0	Updates policy to incorporate changes in technology environments and additional security controls.

Policy Approvals and Reviews:

Date	Organizational Group
3/29/2016	President
3/29/2016	Senior Staff
1/31/2024	Senior Staff Group

Web Links:
Policy Link: www.ut.edu/AUP

Full Policy Text:
Employees are granted use of electronic information systems and network services to conduct University business. 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 technology resources only for authorized purposes.
- Engage in "safe computing" practices, such as setting strong passwords, changing passwords as directed, keeping 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 campus user ID or that originate from their system and/or network wall jacks.
- Use a unique password for your University account(s) that is not used for any personal email accounts, social media, and/or internet sites.
- Complete assigned security awareness training in MyUTampa that is required of all University staff and faculty on a recurring basis, to help prevent phishing email threats and cyber-attacks targeting users.
- 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 accounts assigned to you.
- Ensure that student employees and graduate assistants use **SE** accounts that are created upon request to ITS, rather than their student accounts, when their job duties include the need to access files and folders on the network, or to gain access to enterprise applications. All student employees and graduate assistants using University departmental technology resources are also required to take assigned security awareness training in MyUTampa. *After the hiring process is completed, supervisors need to make a Service Desk request to ITS for their student employee(s) or graduate assistants to take this training (preferably) before the official start date. Additionally, If student employees or graduate assistants will access sensitive or confidential information in emails or departmental folders, they are required to sign a Privileged User Agreement, also available from ITS.*
- Use a University-provided secure file transfer method to share sensitive, private, or confidential information with other internal or external authorized individuals.

- Access only information that is your own, that is publicly available, or to which you have been given authorized access.

Users Should Not:

- Attempt to decode passwords or access control information.
- Disseminate University information without proper authorization.
- Share staff or departmental accounts with student employees or graduate assistants to circumvent the requirement for individual student employee (SE) accounts.
- Use another individual's University-assigned user ID, email account(s), passwords, files, or data without direct delegation or authority provided by this individual.
- Install an enterprise server (providing services to multiple people) unless Information Technology and Security (ITS) pre-approves your request. Servers are only permitted if they do not contain sensitive or confidential data, are properly secured and registered with ITS, and any critical or high-priority security issues identified in University vulnerability scans are promptly remediated by the server administrator.
- Use University systems or networks for personal gain, commercial, illegal, unethical, or partisan political purposes.
- Use your University email account for personal reasons, because on departure from the University, you will lose access to your staff or faculty University email account.
- 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. Do not offer alternate methods of access to UT resources such as personal wifi routers. 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, (preferably) using approved storage methods that the University provides to staff, faculty, and students, such as network folders or internet cloud storage applications such as Dropbox or OneDrive.
- Secure sensitive and confidential information appropriately.
- Control and secure physical and network access to electronic resources and data.
- Properly log out of computer sessions.
- Monitor access to your accounts and promptly *report any suspicion* of unauthorized activity.

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 or remote-control software may be taken off the network without notice if necessary, until the system is reinstalled and the problem is remediated successfully. Users are responsible for contacting ITS immediately if they inadvertently provide their user credentials to unauthorized persons through phishing email links, or other types of internet scams.

Users Should:

- Have current computer/mobile device protection programs (malware prevention, firewalls, etc.) and all operating system updates installed on any computers that are used for University business purposes, prior to connecting them 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 authorized measures to protect the security of technology 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 and Security resources is not private. While the University does not routinely monitor individual usage of technology resources, the normal operation and maintenance of these resources require the backup and caching of data and communications, the logging of activity, monitoring of general usage patterns and other activities necessary for the provision of service.

Every effort is made to ensure the privacy of University of Tampa electronic records. Under rare legal instances or suspected misconduct, the University is obligated to produce information stored on the University network and/or computers and retrieve communications and other records of specific users of UT resources, including individual login sessions and the content of individual communications, without notice.

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:

- Monopolize systems, initiate bandwidth intensive programs, overload networks with excessive data, utilize excessive connect time, disk space, printer paper, color copies, 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:

- In utilizing University technology resources, always respect individuals' rights to be free of intimidation, harassment, and offensive behavior.

Users Should Not:

- Participate in a pattern of conduct when using technology resources that interferes with performing one's assigned role at the University.
- Use email 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 any attempts made by unauthorized persons to gain access to private/protected information.
- Only share University information as appropriate with authorized individuals or agencies.
- Validate email, chat or text requests *directly with the requestor* over the phone or in person if asked to respond to an urgent request to perform an action such as spending personal funds or providing personal information.

Users Should Not:

- Use University systems or networks as a vehicle to gain unauthorized access to other internal or external systems.
- Transmit any electronic communications using a name or email address of someone other than your own assigned computer or account user ID or email 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 utcio@ut.edu.

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 electronic resources at any time following announcement or publication of such change.