Acceptable Use Policy

Document Number: ITS-0001

Date Published(sys): 4/27/2022

General Description

Policy Summary:

This policy outlines the acceptable use of critical people-facing technologies at Trinity. Inappropriate use of computer equipment and people-facing technologies exposes the University to risks including virus attacks, compromise of network systems and services, and legal issues.

Purpose:

The purpose of this policy is to outline the acceptable use of critical people-facing technologies at Trinity University.

Inappropriate use of computer equipment and people-facing technologies exposes Trinity University to risks including virus attacks, compromise of network systems and services, and legal issues. Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of Trinity University's system components, software and data / information.

The hardware, software, and data that constitute the University's information and technology resources are vital to the operation of the university and the fulfillment of its mission. All members of the Trinity University community who use the University's information and technology resources must use them in an ethical, responsible, and legal manner.

Scope:

The Acceptable Usage Policy applies to the Trinity University community (hereafter, the University community) using Trinity University's computer systems, networks, and data systems. The University community includes faculty and staff members, students, alumni, guests, and contractors.

This policy and supporting procedures are applicable to all system components that are owned, operated, maintained, and controlled by Trinity University and all other system components, both internally and externally, that interact with these systems.

- Internal system components are those owned, operated, maintained, and controlled by Trinity University and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other system components deemed in scope.
- External system components are those owned, operated, maintained, and controlled by any entity other than Trinity University, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the description of "Internal system components".
- Trinity University will follow due-diligence best practices by obtaining all relevant information ensuring that other organizations (external to TU) systems components are safe and secure, although Trinity University does not have the ability to provision, harden, secure, or deploy it.

Exceptions:

In a few instances, Trinity systems may require to be exempted from the Acceptable Use Policy due to possible technical difficulties or third-party contractual obligations. Any such exceptions to the current policy must be documented and approved via the Trinity's Exceptions Management Process.

Policy Content

Roles & Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees, and users of system components, along with vendors, contractors, and other relevant third parties.

Additionally, by being aware of one's roles and responsibilities as it pertains to Trinity University information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

- Management Commitment: Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The CIO is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems.

- Internal Employees and Users: Responsibilities include adhering to the organization’s information security policies, procedures, practices, and not undertaking any measure to alter such standards on any Trinity University system components. Additionally, end users are to report instances of non-compliance to this policy to senior authorities, specifically those by other users. End users, while undertaking day-to-day operations, may also notice issues that could impede the safety and security of Trinity University system components and are to also report such instances immediately to senior authorities.
- Vendors, Contractors, Workforce: Responsibilities include adhering to the organization’s information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.
- System/network Administrators: Responsible for the technical implementation and management of the Information Security Policy. They are responsible for certain aspects of system security, such as adding and deleting user accounts, as authorized by the asset owner, as well as normal operations of the system in keeping with job requirements. To ensure system and data integrity, system and network administrators monitor: controlling system access and maintaining current authorization levels for all users; restricting access to sensitive data and maintaining a rigorous authentication practice; documenting system/network administration procedures, parameters, and maintenance activities; creating and maintaining a disaster recovery plan with contingency strategies for dealing with occurrences such as natural disasters, power outages, server failure, virus attacks, and other emergency situations; testing software updates, security controls, and disaster recovery procedures

Policy

Trinity University is committed to ensuring that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management.

Trinity University has developed and implemented comprehensive Usage policies for critical people-facing technologies, which encompass the following categories and supporting activities. These policy directives and supporting procedures will be fully enforced by Trinity University for ensuring the usage policies for critical employee-facing technologies are executed in a formal manner and on a consistent basis for all system components and all other IT resources deemed critical by Trinity University.

Data, software, network capacity, and computer systems have value and must be treated accordingly. Use of IT systems that are shared by many users imposes certain additional obligations. Each member of the University community is personally responsible for their use of these information and technology resources.

Acceptable use of data, software, computers, or network systems does not extend to whatever an individual can do with it. Although some rules may be built into the system itself, these restrictions cannot limit completely what an individual can do or can see. In any event, each member of the community is responsible for his/her actions whether rules are built in, and whether they can be circumvented. An attempt to engage in a prohibited activity is considered a violation whether the attempt is successful or not.

Systems causing network disruption or are deemed to be a security and/or privacy risk may be taken off the network or be otherwise limited without warning. Information Technology Services may employ automated systems that partition or restrict network bandwidth, protocols, or access either internally or at the Internet gateway. The University reserves the right to remove or limit access to material posted on university-owned or administered systems or networks when University policies, contractual obligations, or state or federal laws are violated. Further information is available in the *ITS-0017 TUNetwork Use Policy*.

The University provides computers, software, and network equipment for use by the University community. Trinity University retains ownership and reserves the right to add, remove, upgrade, and replace hardware and software on those systems as deemed necessary by Information Technology Services.

General Use and Ownership

Trinity University proprietary information stored on electronic and computing devices whether owned or leased by Trinity University, the employee or a third party, remains the sole property of Trinity University. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

- Users have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Trinity University proprietary information.
- Users may access, use, or share Trinity University proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Users are responsible for exercising good judgment regarding the reasonableness of personal use.
- For security and network maintenance purposes, authorized individuals within Trinity University may monitor equipment, systems, and network traffic at any time, refer to *ITS-0013 Information Security Policy* for more details.
- Trinity University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Explicit Management Approval to Use the Technologies

Due to the abundance of technologies afforded by today’s technology environment, Trinity University requires explicit management approval for the use of these technologies in conjunction with one's professional roles and responsibilities. The phrase, explicit management approval, consists of the following approval mechanisms and initiatives for the technologies listed below, along with an explicit Usage policy for each respective technology:

Technologies	Management Approval Process	Usage Policy
Network Devices	All system administrative users of network devices (i.e. Firewalls, Routers, Switches, Load Balancers, Intrusion Detection Systems) and other related network devices must gain ITS management approval.	• Network components may not be added, removed, or modified unless explicit consent is granted by appropriate personnel. • Any network devices obtained without proof of purchase and licensing rights will not be allowed onto the network. • All users (system administrative users) must be responsible for the proper use of these devices. • All network system administrative rights and subsequent activities are subject to audit and review as needed.

Technologies	Management Approval Process	Usage Policy
Operating Systems	All system administrative users and end-users of operating systems (Windows, UNIX, LINUX) and other related operating systems must gain ITS management approval to use these systems devices.	• Operating systems may not be added, removed, or modified unless explicit consent is given by appropriate personnel. • Any operating system obtained without proof of purchase and licensing rights will not be allowed onto the network. • All users (system administrative users) must be responsible for the proper use of these operating systems. • All system administrative rights and subsequent activities are subject to audit and reviews as needed.

Technologies	Management Approval Process	Usage Policy
Remote Access Technologies	All end-users of remote access technologies (VPN, Remote Desktop Protocols, etc.) must gain ITS management approval to use these remote access technologies.	• Remote access technologies may not be added, removed, or modified unless explicit consent is given by appropriate personnel. • Any remote access technologies and their supporting protocols obtained without proof of purchase and licensing rights will not be allowed onto the network. • All end-users must be responsible for the proper use of these technologies. • Automatic disconnect of sessions for remote access technologies after a specific period of inactivity is required. • Activation of remote access technologies used by vendors occurs only as needed and will be deactivated after authorized use. • All end users and subsequent activities are subject to audit and reviews as needed.

Technologies	Management Approval Process	Usage Policy
Wireless Technologies	All wireless technologies (Wi-Fi/hotspots) must gain ITS Management authorization prior to being implemented.	• Wireless technologies may not be added, removed, or modified unless explicit consent is given by appropriate ITS personnel. • Any wireless technologies obtained without proof of purchase and licensing rights will not be allowed onto the network. • All end-users must be

		responsible for the proper use of these technologies. - All end users and their subsequent activities are subject to audit and reviews as needed.

Technologies	**Management Approval Process**	**Usage Policy**
Removable Electronic Media	No management approval required	- All users must be responsible for the proper use of these technologies. - Users are prohibited from copying, moving or storage of cardholder data onto local hard drives and removable electronic media when accessing such data via remote access technologies

Technologies	**Management Approval Process**	**Usage Policy**
Desktops	No management approval required	- Trinity owned desktop computers may not be added, removed, or modified unless explicit consent is given by appropriate ITS personnel. - All end-users must be responsible for the proper use of these technologies.

Technologies	**Management Approval Process**	**Usage Policy**
Laptops	No management approval required	- Any Trinity owned laptop obtained without proof of purchase and licensing rights will not be allowed onto the network. - Trinity owned laptops must not

		be added, removed, or modified unless explicit consent is given by appropriate ITS personnel. • All end-users must be responsible for the proper use of these technologies. • Users must protect their Trinity issued laptop from loss, theft, and damage, and must also report loss or theft to the Risk Management and ITS Department in a timely manner..
Technologies	**Management Approval Process**	**Usage Policy**
Internet Use	All users accessing the Internet via the Trinity University network must gain access to use this technology via the formalized and documented process.	• The internet is to be used for business purposes but may be used for personal necessities from time to time. • Connections to the internet are to be conducted through Trinity ITS approved technologies and resources only. • Users may not use the internet to facilitate personal financial gain while at work. • Users may not use the internet to incite violence or conduct any other activity deemed criminal in nature.
Technologies	**Management Approval Process**	**Usage Policy**

Email Use	All users of Trinity University email must gain access to use this technology via the formalized and documented process.	• Email is to be used for business purposes but may be used for personal necessities from time to time. • Connections to the internet for the use of email are to be conducted through company-approved technologies and resources only. • No insecure ports, protocols or services are to be used for email activities. • Users are not allowed to send or receive offensive material via email including, but not limited to pornography and other material deemed offensive in nature. • Users may not use email to facilitate personal financial gain while at work. • Users may not use email to incite violence or conduct any other activity deemed criminal or offensive in nature. • Multi-Factor Authentication MFA for Faculty and Staff is mandatory. •

General Guidelines and Responsibilities

Members of the University community are expected to follow certain principles of behavior in making use of data, computers, and network systems. Members of the University community must:

- Use resources supplied for purposes which are consistent with the business and mission of Trinity University.
- Use the University's computing facilities and information resources, including data, hardware, software, and computer accounts, responsibly and appropriately.
- Respect the rights and property of others.
- Comply with all applicable federal, state, and local laws and University policy.

- Comply with all contractual and license agreements.
- Accept personal responsibility for the proper use of individual accounts and all activity associated with them.
- Safeguard equipment and data entrusted to them (Please refer to the Data Management Policy on appropriate safeguards for protecting student information)

Unacceptable Use and Behavior

Information Security Considerations

Members of the University community are expected to respect restrictions on authorized access to network information and resources. Members of the University community must not:

- Share accounts, passwords, or another computer or network authentication. See *TUNetwork Security Policy* and *Password Policy*.
- Use another user's password (with or without their knowledge).
- Employ a false identity, either directly or by implication, when using an account or other network resources.
- Attempt to gain access to information or resources for which as user does not have explicit authorization.
- Give another individual the means to access data or resources they are not authorized to access.
- Obtain, possess, use, or attempt to use passwords or other information about someone else's account.
- Use any means to view, intercept, or alter data or network traffic not intended for their viewing or use. This applies to data or information stored in or transmitted across computers and network systems, even when that data or information is not securely protected.
- View, copy, disclose, or modify any files or data that do not belong to them, or to which they do not have specific permission.
- Tap phone or data lines or access data by circumventing privacy or security restrictions

Legal Issues / Considerations

Members of the University community are expected to use systems for authorized purposes only. Members of the University community must not:

- Violate copyright as in downloading, recording, or taping of entertainment media without payment of fees or permission of copyright holder.
- Use the University's computing resources for commercial purposes not related to the University's academic, research, and scholarly pursuits.

- Use any IT systems in a way which suggests University endorsement of any political party, candidate, or ballot initiative. This includes e-mailing political messages to any list service maintained by the University which is not explicitly purposed for the posting of political messages.
- Participate in activities that violate state or federal law

Ethical Considerations

Members of the University community are expected to treat all information and technology resources with care and are expected to utilize all resources in ways that respect other users. Members of the University community may not:

- Use computing or network resources to harass, threaten, or otherwise cause harm to others. Discriminatory, demeaning, or abusive behavior may be subject to the University's Policy Statement on Harassment as described in the Faculty and Contract Handbook or the Student Conduct Polices on Respect for Self, Others, and the Community, Respect for Property, Personal Responsibility, or Harassment as described in the Student Handbook.
- Interfere with the proper functioning of the University wired or wireless network. Users may not perform service denial attacks and users may not install their own network equipment on campus. See *ITS-0017 TU Network Security Policy*.
- Use University systems to distribute, produce, publish, view and/or sell obscene or illegal content.
- Deliberately slow a system.
- Release a virus, worm, or other malware.
- Perpetrate fraud, phishing, sniffing, spamming, or unauthorized data mining.
- Members of the University community also are expected to follow all other policies, rules, or procedures established to manage data, computers, or network systems, including those established to control access to, or the use of, computer data, files, or other information. Those who cannot accept these standards of behavior will be denied use of Trinity computers or network systems. Violators may also be subject to penalties under University regulations and under state and federal laws.

Peer to Peer File Sharing Considerations

Using peer to peer (P2P) file sharing applications to illegally share copyrighted music and movies is the #1-way students violate federal copyright law. Students, faculty, and staff are all obligated to comply with federal law and University policy regarding acceptable use of information technology and copyright. The University cannot protect you against allegations of copyright infringement.

First, you will receive a "Take Down Notice" via email requesting that the file sharing program(s) as well as the shared music, film, television and/or game files be removed from your server. You also will communicate with Trinity's Copyright Officer (Jason Hardin, Library) who will provide you with additional educational support.

Failure to complete these sanctions or subsequent violations will result in referral to the Conduct Board.

If you need help removing file sharing software or have questions about P2P file sharing, please call Information Technology Services (ITS) at 210-999-7409 or send e-mail to ITSupport@trinity.edu .

Responsible Use: Employee Personal Use

Employees are provided computing, networking, and information resources as tools to be utilized in the support of University's mission. Employees assume responsibility for appropriate usage and are responsible for exercising good judgment regarding the reasonableness of personal use. Personal use is defined as use that is not job related. In general, incidental, and occasional personal use of the University’s computing systems, including the Internet, is permitted if the personal use does not interfere with the employee’s normal work duties, productivity, or work performance and does not adversely affect the efficient operation of the University’s systems and networks. Individuals are expected to be careful, honest, responsible, and civil in the use of computers and networks. Employees must respect the rights of others, respect the integrity of the systems and related resources, and use these resources in strict compliance with the law, university policies, and contractual obligations.

Using IT resources in the work environment in a manner that results in inappropriate conduct will be addressed as an employee performance issue, even if such conduct does not rise to the level of a university policy violation. Any use of university computers and networks by employees that is inappropriate (such as conducting personal business) to the workplace, or otherwise contributes to creating a harassing or uncomfortable workplace, or creates a legal risk, will subject the employee to counseling, formal disciplinary action and/or termination. Such performance concerns should be directed to the supervisor or the unit Human Resources representative

Performance Evaluation

Consequences of Policy Violation:

Enforcement

To ensure adherence to the Information and Technology Responsible Use Policy and to protect the integrity of University resources, Trinity University reserves the right to monitor the network and computers attached to it. In addition, Trinity University shall have the authority to examine files and account information, and to test passwords, to protect the security of the University's information, network, computing resources and its users.

Any behavior in violation of this policy is cause for disciplinary action. Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources. Sanctions as a result of violations of this policy may result in, but are not limited to, any or all of the following:

- Attending a class or meeting on responsible use issues, as well as successful completion of a follow up quiz;
- Loss of University computing, e-mail and/or voice mail privileges;
- Disconnection from the residential hall network;
- University judicial sanctions as prescribed by the student Code of Conduct;
- Reassignment or removal from University housing and/or suspension or expulsion from the University;
- Prosecution under applicable civil or criminal laws.

Reporting Violations

Reports of problems or violations should be made through the Campus Conduct Hotline, which is a confidential, anonymous way to alert administrators of unsafe or unethical behavior. Phone (866) 943-5787 or report online at Lighthouse Anonymous Reporting .

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Application	Any data entry, update, query, or report program that processes data for the user.
Denial-of-Service Attack (DoS)	An act initiated by a person or people using any electronic means to cause computer resources to become unavailable to its intended users for any length of time.
Host	A computer or IT device (e.g., router, switch, gateway, firewall). Host is

Term:	Definition:
	synonymous with the less formal definition of system.
Information and Technology Resources	The full set of information technology devices (telephones, personal computers, printers, servers, networking devices, etc.) involved in the processing, storage, accessing, and transmission of information owned by, controlled by, or contracted to Trinity University. Connection of these devices can be permanent, via cable, or temporary, through telephone or other communications links. The transmission medium can be physical (e.g., fiber optic cable via Fiber To The X, FTTX) or wireless (e.g.. satellite, wi-fi, Wi-Max).
Operating System	The master control program that runs a computer.
Phishing	The process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.
Sniffing	Employing a program that monitors and analyzes network traffic, to capture data being transmitted on a network.
Spamming	The process of sending unauthorized bulk messages.
System	A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operating environment. When not used in this formal sense, the term is synonymous with the term "host". The context surrounding this word should make the definition clear or else should specify which definition is being used.
System Administrator	A person who manages the technical aspects of a system.
System Owner	Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system.
University Community	Includes faculty and staff members, students, alumni, guests, and contractors.

Related Documents

Related Documents:

Document Type:	Document Name:	Document Number:
Policy	TUNetwork Use Policy	ITS-0017
Policy	Information Security Policy	ITS-0013
Policy	Password Policy	ITS-0015

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v3.0	4/27/2022 11:27 AM	Ben Lim
v2.0	3/16/2022 11:14 AM	Dan Carson
v1.0	8/13/2019 5:07 PM	Courtney Cunningham

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer