TUNetwork Use Policy

Document Number: ITS-0017 **Date Published(sys):** 4/27/2022

General Description

Policy Summary:

This policy is intended to protect the integrity of the campus network, to mitigate the risks and losses associated with security threats to computing resources, and to ensure secure and reliable network access and performance for the University community.

Purpose:

The purpose of this policy is to establish the technical guidelines for IT Network security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the University's comprehensive set of security policies. However, this policy purposely avoids being overly specific to provide some latitude in implementation and management strategies.

Scope:

This policy applies to all users of the Trinity University computing network. Use of the TUNetwork constitutes the user's acceptance of this policy. The Trinity University community (hereafter described as the "University community") includes faculty and staff members, students, alumni, guests, and contractors.

This policy and supporting procedures encompass 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 few instances, Trinity systems may require to be exempted from the Network Security 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

1 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 for such individuals and organizations are much like those stated for end users: 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. System and network administrators measure to ensure system and data integrity include: 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.

② Policy

Trinity University has the responsibility to protect valuable network resources and the confidentiality of sensitive personal information from all threats. In keeping with this responsibility, Trinity University scans network devices connected to the TUNetwork for key security vulnerabilities. Where sufficient cause has been found to indicate a threat to the TUNetwork, a threat to the University or a violation of federal or state law, Trinity may disable the network access of the offending hardware device. Any attempt by a user to circumvent the system or process of scanning for key security vulnerabilities is a violation of this policy.

In keeping with this responsibility, Trinity University has also developed the following policies that relate to virtual private network (VPN) access, bandwidth, disruptive network devices, guest access, TUNetwork services, and devices connected to the TUNetwork.

Bandwidth

Bandwidth refers to the speed of the University's connection to the Internet and is a shared resource in the University community. It is important that members of the University community act responsibly so that this resource is available to everyone, and that the actions - intentional or not - of a few do not disrupt or impede the availability of the Internet for others. Attempts to circumvent, damage, disable or tamper with any system to use more bandwidth or alter how bandwidth is managed or allocated by the Information Technology Service (ITS) is a violation the *TUNetwork Security Policy* and the *Acceptable Use Policy*.

Network Devices & Wireless Access Points

- Network service connections must be approved prior to any connection being made.

- Any exceptions to the established process must be approved by the Chief Information Officer (CIO) or designee. This includes the advance review and approval of all design and engineering specifications involving or affecting university networks by Information Technology Services to confirm compliance with applicable University policies and industry standards.
- The purchase of any computer related device with University funds that will require a network connection must be approved first by the Chief Information Officer (CIO) or designee.
- Personal wireless access points or any other unapproved network device are NOT permitted on the Trinity University network as they can interfere with the wireless network. If found, these devices will be removed and confiscated without notice.
- Information Technology Services retains the right to disconnect and/or block any device from the network without notice if it is determined by ITS that the device is causing bandwidth or any other problems on the Trinity network or if the device has known security vulnerabilities that have not been corrected by maintenance, service releases, and/or security patches. The University deploys software agents to monitor or inventory University-owned devices as well as to perform vulnerability scans on any device connecting to the network.
- ITS ensures that all computers and other devices capable of running antivirus and/or anti-malware software have Trinity-licensed antivirus software installed. ITS ensures that the most recent security patches are installed on each system as soon as practical to adhere to security standards. Where machines cannot be patched, other actions are taken to secure the machine appropriately.
- Connecting devices to the network by means of unauthorized access to University equipment / cabling rooms is prohibited.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, 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 Trinity University.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Trinity University or the end user does not have an active license is strictly prohibited.
- Accessing Trinity University data, servers, or user accounts for any purpose other than conducting Trinity University business, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of national, international, or regional export control laws, is illegal. The

appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others.
- Using a Trinity University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the users.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- 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 duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior authorization has been granted by the Information Technology Services Department.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the Trinity University network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet / Intranet / Extranet.
- Providing information about, or lists of, Trinity University employees to parties outside Trinity University without review and approval of the Information Technology Services Department.

Virtual Private Network

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to access the TUNetwork from off-campus. Trinity University's VPN server is designed to provide off-campus access to TUNetwork resources available on the Trinity campus.

- ITS Core Infrastructure does not recommend the use of TU VPN Server to access Internet resources that are external to Trinity University.

- VPN access is provided to employees with demonstrated need for remote access resources internal to the TUNetwork.
- VPN gateway/concentrators will be set up and managed by ITS. VPN access is available using University owned and approved laptops installed with a VPN client distributed by ITS. All requests for this service must be made by completing the VPN Access Request Form and approved by ITS. This form is available via the University ITS Technology Support Services team.
- By using the VPN technology, employees must understand that University laptops are a de facto extension of the TUNetwork, and as such are subject to the same rules and regulations that apply to University computers on campus.
- Users of this service are responsible for procurement and cost associated with acquiring basic Internet connectivity, and any associated service issue.
- VPN access is controlled using an ID and password issued by the University for authentication.
- All VPN services are to be used solely for the approved business and/or academic support purpose. All users are subject to auditing of VPN usage.
- Disk encryption software will be installed on the laptop to safeguard information stored on the laptop.
- Current VPN software is available for Windows, Mac OS and Linux operating systems.
- All computers connected to the TUNetwork via VPN must use the University approved virus software and are subject to scanning before establishing a connection.
- Users with remote access privileges to TUNetwork must not use non-Trinity University email accounts (e.g., Gmail, Hotmail, Yahoo, AOL), or other external resources to conduct TU business, thereby ensuring that official business is never confused with personal business.

Computing Lab Access

Trinity University maintains computing labs for academic, instructional, research, administrative, and public service purposes. The following guidelines ensure that the computing labs are kept functioning at an optimal level of effectiveness for all users:

- University computer labs must be used in a manner consistent with the policies of Trinity University
- All persons using the lab are responsible for backing up their own data and protecting their own information.
- Printing from lab machines can be sent to a print station. A Trinity University Tiger Card or guest print card will need to be purchased to be able to print.
- Food, beverages, tobacco use, weapons, firearms, or animals, except service animals, are prohibited in the computing labs.

- Audio output or sound playing devices are permitted only with the use of headphones.
- Use of two-way communication devices are prohibited in the labs. Ringers and alarms on these devices should be turned off or set to vibrate while in the labs.
- Children are permitted in labs only if accompanied by Trinity University faculty, staff or students.
- ITS lab equipment may not be used for personal business purposes or in any for-profit venture.
- Disabling computers by disconnecting cables, removing hardware, applying software locks or locking workstations will be considered vandalism and treated as such under the University policy.
- ITS employees, including ITS student workers, are responsible for maintaining order in the labs. Anyone violating these policies, or disturbing others in any way, will be asked to leave.
- Persons with special needs requiring special access to computer laboratory equipment may contact the Coordinator of Disability Services (dss@trinity.edu / 210- 999-7411).

Guest Users

Trinity University provides wireless Internet access for visitors and guests. Wireless access is available in most public areas of the campus. To access the Trinity University wireless network, select TUGuest from the list of wireless networks. Guests must comply with the *Acceptable Use Policy*.

Wireless Networks

Trinity University is to ensure 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:

- Controls and processes are in place to detect and identify unauthorized wireless access points.
- Processes are in place and defined for detecting and identifying all wireless access points on a quarterly basis.
- An inventory of authorized wireless access points is maintained.

Provisioning and Hardening

Initially implementing a WLAN requires adherence to the following stated guidelines for ensuring the safety and security of the wireless platform itself, and that all wireless

access points are included in the change control process (so updates are formally managed), along with ensuring the confidentiality, integrity, and availability (CIA) of Trinity University's overall information systems landscape:

- Secure Deployment: All WLAN devices and supporting resources, such as wireless access points, and other network devices, are to be positioned in a manner for ensuring only authorized access and modification. Additionally, they are to be secured with approved fixtures and other necessary apparatuses for mitigating any unnecessary movement. Additionally, the WLAN platform itself is to be logically | physically segregated from the corporate | internal wired network, which can be achieved by utilizing firewalls and other access control methods.
- Asset Inventory: Once all WLAN devices are safely secured, a complete asset inventory is to be taken, documenting all necessary information, such as physical location, and corresponding unique identifiers (i.e., hostnames, serial numbers, etc.).
- Configuration of Wireless Access Points: The following measures are to be undertaken regarding WLAN platforms:
    - Change default administrator settings, such as username and password, along with implementing strong, unique administrative passwords (i.e., alphanumeric, case sensitive, etc.) for all wireless access points.
    - Change any default IP addresses also.
    - For all remaining services and protocols, implement the concept of "least privileges".
    - Implement MAC Address filtering on wireless access points.
    - Protect all sensitive wireless access points information, such as administrator passwords, SSID password, keys, etc. with approved security measures, such as encryption.
    - Enable logging features and ensure that all logs and audit trails are sent to a remote logging server and retained as necessary (i.e., regulatory compliance laws, etc.). Information captured should include, but not limited to, the following: MAC addresses, user logon information (i.e., time, username, etc.), user logoff information
    - Enable usage parameters, such as time-out sessions.
    - Ensure appropriate network security protocols are in place for helping ensure the overall safety and security of all WLAN platforms. Specifically, for internal, corporate WLAN's, use appropriate layered defense mechanisms, such as firewalls, intrusion detection systems, etc.
- End-User Security: Access to Trinity University WLAN environments requires the use of anti-virus on all laptops, desktops, and other workstations. Additionally, because information often sent via wireless can be deemed sensitive and confidential, all users are to abide by Trinity University wireless security general guidelines, responsibilities, and acceptable user as defined below.

Rogue AP's

Wireless Access Points installed by users onto the organization's WLAN without the knowledge or consent of authorized personnel are deemed "rogue" and are in violation of current policy. Because rouge wireless access points (WAP) have not gone through an extensive provisioning and hardening process, they pose an immediate threat to the safety and security of Trinity University system components and are to be promptly disabled upon being identified. Physically removing the WAP apparatus and/or shutting down connectivity (such as the switch port, blocking an IP address, etc.) are considered acceptable. An approved wireless analyzer – one capable of detecting all wireless access points – is to be used on a regular basis for both confirming all allowed AP's, along with identifying Rogue AP's.

Access Rights

Administrative access rights to Trinity University WLAN platforms are limited to authorized personnel only, such as systems administrators, network engineers - individuals responsible for the overall design, configuration, implementation, maintenance, and monitoring of wireless access points. End user access rights include all employees and other applicable third parties as designated by Trinity University. Additionally, all access must include the user of a username and password for helping prevent unauthorized access to Trinity University wireless local area networks.

Wireless Security Threats

The use of wireless security provides convenience, portability, and flexibility, but also numerous security threats, for which all individuals at Trinity University are to be aware of, such as the following:

- Spoofing: More specifically – MAC spoofing – can occur whereby MAC addresses are obtained by unauthorized parties and used (in conjunction with other software tools) for gaining access to a network.
- Denial of Services (DoS): A concept whereby an attacker deliberately floods a network – in this case, a WLAN platform – with requests and other network related activities, resulting in the loss of use for intended users, and possibly even the platform "crashing".
- Eavesdropping and Tampering: Intercepting, capturing and/or modifying data and information being sent or received over the WLAN platform

Continuous Monitoring

Security for all Trinity University WLAN platforms is highly dependent on comprehensive continuous monitoring practices, such as the following:

- Changing administrator wireless access points passwords every ninety (90) days.
- Changing end-user wireless access points passwords every ninety (90) days.
- Updating of firmware and related patches and security updates as necessary.
- Reviewing all log files on a regular basis and reporting issues, concerns, constraints immediately.
- Reviewing access rights on a regular basis, both administrator access rights, along with end-user access rights.
- When making any configuration changes to the WLAN platforms, it is to be conducted by authorized personnel only, and fully documented in accordance with Trinity University change management policies and procedures.
- Actively scanning on a regular basis for Rogue AP's and immediately disabling such platforms.
- When disposing of wireless access points devices, remove configuration settings relating to network security, passwords, keys, etc.

Security Awareness Training

A strong cyber security program cannot be put in place without significant attention given to training to Trinity University IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. In addition, those in Trinity University who manage the ITS infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because security of Trinity University resources is as much a human issue as it is a technology issue.

An important component of security is training all Trinity University employees and other applicable users of relevant security measures and precautions pertaining to use of technology and industry best practices

All faculty, students and staff who will be required to attend cyber security awareness training on an annual basis.

Testing and Approval of Network Changes

- The Core Infrastructure Team tests and approves all network connections and changes to firewall and router configurations, before moving to the production environment.
- Any changes to such processes and procedures must be reviewed and approved by authorized personnel at Trinity University for ensuring such changes still meet the needs of the organization along with any other sensitive and confidential information being stored, processed, and/or transmitted

Performance Evaluation

Consequences of Policy Violation:

Enforcement

To ensure adherence to the *TUNetwork Security Policy* and to protect the integrity of university resources, the University reserves the right to monitor the network and computers attached to it.

Non-standard software on University-owned devices will be removed as part of a normal repair process if necessary to restore system functionality. In the event of computer or network performance issues associated with a computer enabled with administrator level access, ITS will only restore the computer to the standard configuration for all University computers. The occurrence of repeated instances of OS integrity problems may result in the removal of administrator level access in order to prevent continued challenges in supporting the computer.

Anyone who changes a MAC address, IP address, or netid with the intention of disguising or forging his or her identity may be in violation of University policy.

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 because of violations of this policy may result in, but are not limited to, any or all the following:

- Attending a class or meeting on network use issues, as well as successful completion of a follow up quiz.
- Loss of University computing, email and/ or voice mail privileges.
- Disconnection from the residential hall internet 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 law.
- Employees may be subject to disciplinary action, .

- Violation of policies in regard to the computers in the computer labs may result in loss of computer lab privileges and other disciplinary action as described in the various handbooks issued by the University to students, faculty, and staff.

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:
Administrator access	This level allows the user to have complete and unrestricted access to the computer. This includes the ability to install any hardware or software, edit the registry, manage the default access accounts and change file level permissions. Manipulating these may cause serious stability issues with the computer system.
General access	This level allows most administrative powers with some restrictions. Installation of software or hardware that makes changes to the underlying operating system will require the assistance of ITS. General Access Level will generally assure the highest level of stability for a computer.
Host	A computer or IT device (e.g., router, switch, gateway, firewall). Host is 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) or wireless (e.g.. satellite, wi-fi, WimAX).
Operating System	The master control program that runs a computer.
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.

Term:	Definition:
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.
Virtual Private Network (VPN)	A method for accessing a remote network that uses encryption and tunneling to connect users securely over a public network, usually the Internet.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v4.0	4/27/2022 11:29 AM	Ben Lim
v3.0	3/16/2022 10:43 AM	Dan Carson
v2.0	8/21/2020 8:02 AM	Holly Warfel
v1.0	8/14/2019 5:16 PM	Courtney Cunningham

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer