TUNetwork Use Policy

General Description

Purpose:
The hardware and software that constitute Trinity University’s computing network are vital to the operation of the university. Viruses, malware, computer vulnerabilities and inappropriate use of the TUNetwork are a threat to these resources and can detrimentally affect the ability to accomplish the institution’s mission. Trinity University has a responsibility to maintain these resources and ensure they are used in an appropriate manner. The TUNetwork Use Policy addresses this responsibility.

Scope:
The TUNetwork Use 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.

Policy Content

Summary

Trinity University has the responsibility to protect valuable network resources and the confidentiality of sensitive personal information from any and all threats. In keeping with this responsibility, Trinity University scans computer hardware 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 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 in order to use more bandwidth or alter how bandwidth is managed or
allocated by the Information Technology Service (ITS) is a violation the TUNetwork use Policy and the Information and Technology Responsible Use Policy.

**Disruptive Network Devices**

- 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 in order 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 will deploy software agents to monitor or inventory University-owned devices as well as perform vulnerability scans on any device connecting to the network.

ITS will ensure that all computers and other devices capable of running antivirus and/or anti-malware software have Trinity-licensed antivirus software installed. ITS will ensure 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 may need to be taken to secure the machine appropriately.

Connecting devices to the network by means of unauthorized access to University equipment/cabling rooms is prohibited.

**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.
Using the VPN server to access Internet resources external to Trinity University is not recommended.

VPN access is provided to employees with demonstrated need for remote access resources internal to the TUNetwork.

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 Help Desk.

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.

• VPN gateway/concentrators will be set up and managed by ITS.

• Users of this service are responsible for procurement and cost associated with acquiring basic Internet connectivity, and any associated service issue. VPN services work best over broadband connections (xDSL or FTTx).

• It is the responsibility of the employee with VPN privileges to ensure that unauthorized users are not allowed access to the TUNetwork.

• 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.

• VPN users may be automatically disconnected from the TUNetwork after fifteen minutes of inactivity.

• Disk encryption software will be installed on the laptop to safeguard information stored on the laptop.

• Current VPN software is available for Windows and Mac OS.

• 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 must ensure that their University-owned computer or workstation that is remotely connected to TUNetwork is not also connected to any other network at the same time.

• 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.

**Administrator Access**

Trinity University is committed to providing members of the University community with reliable technology and stable operation conditions while appropriately addressing the University needs for system integrity and data security. By default, all Trinity Faculty/Staff members are assigned general access level rights on their individual workstations. Exceptions may be granted to Faculty/Staff members who require Administrator level access to perform job related tasks. Individuals may request
administrator level access through the ITS HelpDesk (helpdesk@trinity.edu or x7409) and sign the Request for Administrator Access document (provided by ITS), acknowledging that they have read all applicable IT policies. Users who are granted “administrator” access on University owned computers or workstations have enhanced responsibilities governed by the following policies:

- Trinity University workstations are university property and are intended for university business only.

- Individuals should only install software related to university business.

- Individuals should not install software that may damage files and expose TUNetwork to virus attacks and malicious coding.

- Individuals should refrain from installing software which may monopolize local processor power, resulting in noticeable system slowdown or degradation of performance.

- Individuals should not install applications that may establish network share protocols, which result in an increase in bandwidth utilization as this may cause network congestion and degradation of network performance across wide areas of the campus.

- Individuals should not download or install applications (software) that are illegal or not licensed on university-owned equipment.

- Individuals who download or install applications (software), other than those included in the standard configuration for all university computers, are responsible for retaining documentation of appropriate licenses. Individuals are also responsible for re-installing this nonstandard software if necessary.

Trinity IT Services is charged with creating a central network registry service. This service maintains a current record of all devices connected to the TUNetwork through a continually updated database. This extends to wireless communications. The Trinity IT central network registry service will automatically generate a registration page when a user or systems administrator connects an information technology device to the TUNetwork. The user or systems administrator must complete this page before the device is operated on the TUNetwork. The page requires the MAC address and the IP address (if static) and the network electronic identifier (netid) of the primary user/responsible administrative person. Network administrators are required to register all devices connected to networks under their domains for which individual users or systems administrators, for whatever reason, have not themselves registered. (The development of a guest registry system is not covered under this policy.)

**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:

- Persons using laboratory equipment must have a Trinity University ID card valid for the current semester and must be able to produce the card upon request.

- University computer labs must be used in a manner consistent with the policies of Trinity University including the Responsible Information and Technology Use Policy.

- 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 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 University faculty or staff.

- Whenever others are waiting, computer use is restricted to one-hour sessions.

- Games that are part of class assignments are subjected to the time limits stated above.

- ITS lab equipment may not be used for 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 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. A Wi-Fi certified wireless network card that is 802.11a, 802.11g, or 802.11n compatible is required to access the TUGuest wireless network, a standard for most modern laptops and mobile devices. Guest wireless access allows only for standard Internet surfing (ports 80 and 443), much like that found in many coffee shops. Application connections requiring non-standard ports will not be supported. For example, email connections through a desktop application like Outlook or Thunderbird will typically not work; connect via a Internet browser instead.

Alumni, official guests of the University, parents, and prospective students may be logged on to any available public computer. Services/resources available to guest users are:

- Free internet access with presentation of a photo ID (similar to public libraries)
- Full catalog and database access while in the building or on campus wi-fi

Guests must comply with the Responsible Information and Technology Use Policy.

Performance Evaluation

Consequences of Policy Violation:

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

Any attempt by a user to circumvent the system or process of scanning for key security vulnerabilities is a violation of this policy. 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.

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.

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.

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 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;
- Monetary reimbursement to the University or other appropriate sources;
- 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.

**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 email cch@eiaa.org. Further information can be found at [http://www.campusconduct.com](http://www.campusconduct.com)

**Requirements**

**Approvals:**
Chief Information Officer
### Terms and Definitions:

<table>
<thead>
<tr>
<th>Term:</th>
<th>Definition:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator access</td>
<td>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.</td>
</tr>
<tr>
<td>General access</td>
<td>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.</td>
</tr>
<tr>
<td>Information and Technology Resources</td>
<td>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).</td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td>A method for accessing a remote network that uses encryption and tunneling to connect users securely over a public network, usually the Internet.</td>
</tr>
</tbody>
</table>
Related Documents

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Document Name</th>
<th>Document Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Responsible Information and Technology Use Policy</td>
<td>ITS-0001</td>
</tr>
</tbody>
</table>

Revision Management

<table>
<thead>
<tr>
<th>Revision #:</th>
<th>Date:</th>
<th>Recorded By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>8/14/2019 5:16 PM</td>
<td>Courtney Cunningham</td>
</tr>
</tbody>
</table>