Responsible Information and Technology Use Policy

General Description

Purpose:
Trinity University’s computer systems, network, and data are vital to operations. 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. The Responsible Information and Technology Use Policy addresses this responsibility.

Scope:
The Responsible Information and Technology Use 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.

Exceptions:
None.

Policy Content

Summary
Data, software, network capacity, and computers 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.

Legitimate use of data, software, computers or network systems does not extend to whatever an individual is capable of doing 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 or not rules are built in, and whether or not they can be circumvented. An attempt to engage in a prohibited activity is considered a violation whether the attempt is successful or not.

Systems using excessive amounts of bandwidth, 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 does not monitor or generally restrict the content of material transported across the University's networks or stored on University-owned computers. 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 TUNetwork Use Policy.

The University provides computers, software, and network equipment for use by the University community. The 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 Resources.

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).

Responsible Use - Information Security

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 other computer or network authentication. See TUNetwork Use 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.

**Responsible Use – Legal Issues**

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.

**Responsible Use – 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 Policies 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. In particular, users may not perform service denial attacks and users may not install their own network equipment on campus. See TUNetwork Use 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.

**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 as long as 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;
- 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 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 email cch@eiia.org. Further information can be found at 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>Denial-of-Service Attack (DoS)</td>
<td>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.</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 via Fiber To The X, FTTX) or wireless (e.g., satellite, wifi, Wi-Max).</td>
</tr>
<tr>
<td>Phishing</td>
<td>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.</td>
</tr>
<tr>
<td>Sniffing</td>
<td>Employing a program that monitors and analyzes network traffic, to capture data being transmitted on a network.</td>
</tr>
<tr>
<td>Spamming</td>
<td>The process of sending unauthorized bulk messages.</td>
</tr>
<tr>
<td>University Community</td>
<td>Includes faculty and staff members, students, alumni, guests, and contractors.</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>TUNetwork Use Policy</td>
<td>ITS-0017</td>
</tr>
<tr>
<td>Policy</td>
<td>Information Security Policy</td>
<td>ITS-0013</td>
</tr>
<tr>
<td>Policy</td>
<td>Password Policy</td>
<td>ITS-0015</td>
</tr>
</tbody>
</table>

Revision Management

Revision History Log:

<table>
<thead>
<tr>
<th>Revision #:</th>
<th>Date:</th>
<th>Recorded By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>8/13/2019 5:07 PM</td>
<td>Courtney Cunningham</td>
</tr>
</tbody>
</table>