☑ Policy Name – Acceptable Use	Effective Date: As of date signed	Policy Version: 2	Policy Status: Final
Board of Trustees Chairman (when applicable): **Senior Vice President/Executive Vice President:**			
David Raab, Executive Vice President and Chair of the ISSC		**Date: 8/10/17**	
Department Head: Franklin Steen, VP for Technology/CIO		**Date: 8/10/17**	
Patricia Ciuffo, CISO		**Date: 8/10/17**	

I. Purpose

In the interests of learning and research, and to support its academic, research, and administrative functions, Touro College & University System (TCUS) provides students, faculty, and staff with access to computer and network resources. TCUS seeks to promote and facilitate the proper use of Information Technology. However, while the tradition of academic freedom will be fully respected, so too will the requirement of responsible and legal use of the technologies and IT facilities that are made available to faculty and staff. This Acceptable Use Policy (AUP) is intended to provide a framework for the use of TCUS's IT resources and should be interpreted to have the widest application[1]. This AUP addresses the entire TCUS Community.

Institutional technology resources, facilities, and/or equipment include all technology-based resources, facilities, and/or equipment that are owned and/or operated by TCUS as part of its mission. The basic rules for use of the institutional technology resources, facilities, and/or equipment are to act responsibly, to abide by the TCUS's policies as specified in the TCUS Handbooks, and to respect the rights and privileges of other users. Each user of TCUS technology resources is responsible for adhering to all legal and ethical requirements in accordance with the policies of TCUS and applicable law.

TCUS technology resources, facilities, and/or equipment may only be used by TCUS community members as per Touro Employee and Student Policies unless otherwise authorized by the President, Provost or their designated alternates (VP, Dean, or above). Members of the TCUS community may not allow other person(s) to utilize TCUS's technology resources, facilities, and/or equipment.

All users of TCUS IT resources (hereafter referred to as "users") must acknowledge, upon initial employment or promotion, or other appropriate time, the AUP upon signing in to the TouroOne system. A copy of the Policy is also available online. In acknowledging the AUP, each individual will be certifying that he/she has read and will comply with the AUP. This Policy contains elements that intersect with other policies at TCUS. Should there be questions as to which policy applies; requests for clarifications should be addressed, in writing, to the CISO at CISO@Touro.edu.

[1]**IMPORTANT DISCLAIMER**
This policy does not form a contract. Touro College & University System (TCUS) reserves the right to amend, revoke this policy, in whole or in part, at any time, with or without notice in its sole discretion. The policy is neither written nor meant to confer any rights or privileges on an individual or equity or bypass any obligations on TCUS other than its obligations under the law. As with all TCUS policies, this policy is written for informational purposes only, may contain errors and may not be applicable to every situation or circumstance. Any dispute, claim or controversy arising out of, or related to this policy, which is not resolved through TCUS's internal procedures (hereafter, "Disputes") shall be resolved exclusively through final and binding expedited arbitration conducted solely by the American Arbitration Association (AAA), or any successor, in interest in accordance with the AAA Rules than in effect. The location of the arbitration shall be TCUS's main campus.

☑ Policy Name – Acceptable Use	Effective Date: As of date signed	Policy Version: 2	Policy Status: Final
Board of Trustees Chairman (when applicable): **Senior Vice President/Executive Vice President:**			
David Raab, Executive Vice President and Chair of the ISSC		**Date: 8/10/17**	
Department Head: Franklin Steen, VP for Technology/CIO		**Date: 8/10/17**	
Patricia Ciuffo, CISO		**Date: 8/10/17**	

II. Scope

This policy applies to all users (consultants, vendors, volunteers, temps, etc.) of IT resources in all departments of TCUS.

III. Definitions

TCUS – Touro College & University System. This includes all New York campus locations, including NYMC, all California, Nevada, Illinois and all foreign locations.

Touro systems—computer systems owned and operated by Touro as well as Touro licensed cloud-based systems used by Touro employees and students in the course of their employment or studies.

Touro community – identified as members with a TouroOne portal ID or access (e.g., wireless, library, and email) to TCUS IT resources.

IV. Policy and Implementation

TCUS IT resources are provided primarily for academic (including support of research, and laboratory-related activities) and communication purposes to facilitate a person's academic or administrative role (Faculty, Staff, Student) within the TCUS Community. Other uses, such as personal electronic mail or recreational use of the Internet are not rights but privileges, which may be withdrawn. Any such use must not interfere with the user's duties or studies or any other person's use of computer resources and must not, in any way, damage TCUS's reputation.

TCUS-provided email addresses must be used for all official TCUS business to facilitate official TCUS communication, audit ability and institutional record keeping. All individuals in the TCUS community ("members") are obligated to read their TCUS-supplied email, which is considered the official means of communication for TCUS.

AUTHORIZATION

To use the computing resources of TCUS, a person must be a member of the TCUS community. Members will be issued a username, password and email address (nonmember guests will not be issued a TCUS email address). Authorization for other services may be requested by application based on need. Use of TCUS technology resources implies, and is conditional upon, acceptance, via electronic signature, of this Acceptable Use Policy.

☑ Policy Name – Acceptable Use	Effective Date: As of date signed	Policy Version: 2	Policy Status: Final
Board of Trustees Chairman (when applicable): **Senior Vice President/Executive Vice President:**			
David Raab, Executive Vice President and Chair of the ISSC		**Date: 8/10/17**	
Department Head: Franklin Steen, VP for Technology/CIO		**Date: 8/10/17**	
Patricia Ciuffo, CISO		**Date: 8/10/17**	

All individually allocated usernames, passwords and email addresses are for the exclusive use of the individuals to whom they are allocated. The user is personally responsible and accountable for all activities carried out under his/her username. The password associated with a particular username must not be divulged to any other person, and any attempts to access or use any username or email address, which are not authorized to the user, are prohibited. All users must correctly identify themselves at all times. A user must not masquerade as another, withhold his/her identity, or tamper with audit trails. A user must take all reasonable precautions to protect his/her resources. In particular, passwords used must adhere to current password policy and practice.

PRIVACY

TCUS sees privacy, not regulated by law (such as Family Educational Rights and Privacy Act (FERPA) or Health Insurance Portability and Accountability Act (HIPAA)), as a privilege and not an absolute right. Therefore, members should not hold or pass information that they would not wish to be seen by staff responsible for their administrative or academic-related work.

After a member of the TCUS community leaves TCUS, files left behind on any computer system owned by TCUS, including servers, cloud based services and electronic mail files, will be kept for a period consistent with record retention policies of TCUS and then destroyed. Records maintained on TCUS's systems, including cloud based systems, are the sole and exclusive property of TCUS and no privacy right attaches to such records and those records may be viewed by authorized personnel with a need to know within the Institution even if they are otherwise privileged.

ACCEPTABLE USE

Use of Technology resources is expected for academic (teaching, research including laboratory), administrative, and communication purposes. Acceptable use of TCUS IT resources may be summarized as follows:

- Users are required to abide by all intellectual property, copyright or similar laws or regulations. Plagiarism, in any form, is unacceptable at TCUS.
- Conventional norms of behavior apply to IT-based media, just as they would apply to more traditional media. Within TCUS, this would mean that the tradition of academic freedom will always be respected. TCUS, as expressed in relevant handbooks, is committed to maintaining an educational and working environment that provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, sexual orientation, national origin, age, disability or special need.

☑ Policy Name – Acceptable Use	Effective Date: As of date signed	Policy Version: 2	Policy Status: Final
Board of Trustees Chairman (when applicable): **Senior Vice President/Executive Vice President:**			
David Raab, Executive Vice President and Chair of the ISSC		**Date: 8/10/17**	
Department Head: Franklin Steen, VP for Technology/CIO		**Date: 8/10/17**	
Patricia Ciuffo, CISO		**Date: 8/10/17**	

- All users of TCUS technology services must not disable anti-virus or automated mechanisms that update virus signatures or prevent security patches on workstations from being applied; all workstations must be adequately protected against viruses and malware, through the use of up-to-date anti-virus software with the latest tested security patches installed. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.
- Users of services external to TCUS are expected to abide by any policies, rules, terms of service or use, and codes of conduct applying to such services. Any breach of such policies, rules, terms of service or use, and codes of conduct that are reported to TCUS may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. The use of TCUS credentials to gain unauthorized access to the facilities of any other organization is similarly prohibited.

UNACCEPTABLE USE

Use of Technology resources to interfere with the business of TCUS is unacceptable. Unacceptable use of TCUS IT resources include, but are not limited to, the following actions:

- Distributing materials which are offensive, obscene, defamatory or abusive. Such material may be illegal and violate TCUS policies on abuse. Users of TCUS computer systems must be familiar with, and comply with, TCUS abuse policies.
- Interfering or attempting to interfere in any way with information belonging to or material prepared by another user. Similarly, no user shall make unauthorized copies of information belonging to another user.
- Intellectual property rights infringement, including copyright, trademark, patent, and piracy is unacceptable. It is unacceptable to download, distribute, or store music, video, or other material for which you do not hold a valid license or other valid permission from the copyright holder.
- Use of TCUS email to solicit anyone for donations to a charitable cause or to purchase goods or services of any kind, not connected to TCUS or the job duties of the employee, or to participate in any activity not sponsored by TCUS, including without limitation, any activity which is political, charitable, social, entertainment, educational, or advocacy, in nature.
- Unsolicited advertising (often referred to as "spam email"), sending emails that purport to come from an individual other than the person actually sending the message (using a forged address), or sending emails that solicit another person's account and password.

☑ Policy Name – Acceptable Use	Effective Date: As of date signed	Policy Version: 2	Policy Status: Final
Board of Trustees Chairman (when applicable): **Senior Vice President/Executive Vice President:**			
David Raab, Executive Vice President and Chair of the ISSC		**Date: 8/10/17**	
Department Head: Franklin Steen, VP for Technology/CIO		**Date: 8/10/17**	
Patricia Ciuffo, CISO		**Date: 8/10/17**	

Note: users who receive unsolicited "spam email" should forward the message to Information.Security@touro.edu for follow up, wherever practical.

- Attempting to break into, gain access to, or damage computer systems or data of TCUS computers or any other computers for which the individual is not authorized, or attempting to facilitate actions to accomplish same.
- Connecting an unauthorized device to TCUS's network, such as one that has not been configured to comply with this policy or with any other relevant regulations and guidelines relating to security, IT purchasing policy, and acceptable use.
- Circumvention of network access controls, monitoring or interception of network traffic, without permission; probing for the security weaknesses of systems by methods such as port-scanning, without permission; associating any device to network Access Points, including wireless, for which you are not authorized.
- Providing any services to others via remote access. The installed machine on each network segment must be a workstation only and not provide any server-based services, including, but not limited to, Web, File Transfer, Streaming Media server, peer-to-peer facilities, or email services.
- Using TCUS systems or networks in a manner that violates TCUS policies or federal, state or local law.
- Use of TCUS systems or networks for commercial purposes unrelated to TCUS.
- Reconfiguring or otherwise adjusting any settings on any TCUS shared computer, device, technology resource, software and/or hardware without explicit permission from the VP for Technology at TCUS or designated staff.
- Elevating a user's access permissions beyond their job responsibilities. TCUS community users are assigned the minimum access rights required to perform job-related duties and responsibilities. For faculty and staff, standard computer user rights allow use of applications and tools needed to complete work tasks in a timely fashion. Computer "administrative rights" are reserved for TCUS IT technology staff as defined by job responsibilities.
- Removing any equipment from TCUS without explicit permission of TCUS Administrative Management.
- Sending student (FERPA-governed) or patient (HIPAA-governed) data via email or storing this type of confidential data on any portable device or virtual space outside of TCUS's administrative control in an unencrypted state.

☑ Policy Name – Acceptable Use	Effective Date: As of date signed	Policy Version: 2	Policy Status: Final
Board of Trustees Chairman (when applicable): **Senior Vice President/Executive Vice President:**			
David Raab, Executive Vice President and Chair of the ISSC		**Date: 8/10/17**	
Department Head: Franklin Steen, VP for Technology/CIO		**Date: 8/10/17**	
Patricia Ciuffo, CISO		**Date: 8/10/17**	

With Respect to Restricted and Confidential TCUS Data, access is allowed solely to members of the TCUS community to perform their job responsibilities. Members of the TCUS community should **not**:

- seek personal benefit or permit others to benefit personally from any Restricted or confidential data that has come to them throughout their work assignments.
- make or permit unauthorized use of any restricted or confidential data in any of the TCUS's computer systems or other records.
- enter, change, delete or add data to any computer system or files outside of the scope of their job responsibilities.
- include or cause to be included in any record or report, a false, inaccurate or misleading entry known to the user as such.
- alter or delete or cause to be altered or deleted from any records, report or information system, a true and correct entry.
- release restricted or confidential data other than what is required in completion of job responsibilities which is consistent with this Policy.
- exhibit or divulge the contents of any record, file or information system to any person unless it is necessary for the completion of their job responsibilities.

Members are strongly encouraged to report any suspected violation of this policy or any other action, which violates confidentiality of data according to the security and incident reporting instructions defined under the security breach section of this policy.

SECURITY BREACHES

A suspected computer breach or security incident represents the attempted or successful unauthorized access, use, modification, or destruction of information systems or data. If unauthorized access occurs, computer systems could potentially fail, and restricted and/or confidential information could be compromised. Thus, it is TCUS's policy that all suspicious activity be immediately reported, especially if the individual has violated this Policy. Additionally, given the potential harm that the TCUS may suffer with the release of any restricted or confidential data all employees are strongly encouraged to report any suspected violation of this policy or any other action, which violates confidentiality of data. Reporting can be done as follows:

☑ Policy Name – Acceptable Use	Effective Date: As of date signed	Policy Version: 2	Policy Status: Final
Board of Trustees Chairman (when applicable): **Senior Vice President/Executive Vice President:**			
David Raab, Executive Vice President and Chair of the ISSC		**Date: 8/10/17**	
Department Head: Franklin Steen, VP for Technology/CIO		**Date: 8/10/17**	
Patricia Ciuffo, CISO		**Date: 8/10/17**	

- Faculty should report the incident to their local campus Dean or Department Chairperson or their local IT Director in writing. A copy should be sent to the Chief Information Security Officer at CISO@Touro.edu.

- Non Faculty should report the incident in writing to their local Manager and their local IT Director. A copy should be sent to the Chief Information Security Officer (CISO) at CISO@Touro.edu.

- All TCUS technology users are required to inform their campus IT Director and the CISO at CISO@Touro.edu of any security vulnerabilities (loopholes) discovered, and to cooperate in implementing any security measures and procedures needed to close these vulnerabilities.

- TCUS technology resource users should not execute any form of network scanning (e.g., port, security) without the express written permission of the CISO who will bring these requests for approval to the Information Security Steering Committee (ISSC).

The CISO will coordinate with TCUS Counsel and Senior Management in reporting computer breaches to law enforcement authorities.

V. Enforcement

All users are required to abide by the policy.

TCUS reserves the right to have access to email, files, history and other utilization and audit trail data or information so as to enable TCUS to monitor equipment, systems and network traffic at any time or to ensure compliance with this Policy and applicable laws.

Any member of the TCUS community found to have violated this Policy may be subject to disciplinary action, according to the applicable TCUS handbook.

No exceptions to this Policy will be granted. Individual requests for modifications from this Policy must be made in writing to the Chief Information Security Officer (CISO) who will consult with appropriate Senior Management, and, if granted, will be acknowledged in writing.

☑ Policy Name – Acceptable Use	Effective Date: As of date signed	Policy Version: 2	Policy Status: Final
Board of Trustees Chairman (when applicable): **Senior Vice President/Executive Vice President:**			
David Raab, Executive Vice President and Chair of the ISSC		**Date: 8/10/17**	
Department Head: Franklin Steen, VP for Technology/CIO		**Date: 8/10/17**	
Patricia Ciuffo, CISO		**Date: 8/10/17**	

VI. Responsibilities

VP for Technology/Chief Information Officer
Chief Information Security Officer

VII. Management

Responsible Officer: CIO and CISO
Responsible Department: Information Technology