ACCEPTABLE USE POLICY

In the interests of learning and research, and to support its academic, research, and administrative functions, Touro provides students, faculty, and staff with access to computer and network resources. Touro 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 is intended to provide a framework for the use of Touro's IT resources and should be interpreted to have the widest application[1]. This Acceptable Use Policy addresses the entire Touro Community.

Institutional technology resources, facilities, and/or equipment include all technology-based resources, facilities, and/or equipment that are owned and/or operated by Touro 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 Touro's policies as specified in the Touro Handbooks, and to respect the rights and privileges of other users. Each user of Touro technology resources is responsible for adhering to all legal and ethical requirements in accordance with the policies of Touro and applicable law.

Touro technology resources, facilities, and/or equipment may only be used by current employees unless otherwise authorized by the Dean of Faculties, the Senior Vice President for Administration, or Senior Vice President and Chief Financial Officer, or their designated alternates. Members of the Touro Community may not allow other person(s) to utilize Touro's technology resources, facilities, and/or equipment.

All users of Touro IT resources (hereafter referred to as "users") must sign, upon initial employment or promotion, or other appropriate time, the Acceptable Use Policy (AUP), and submit the signed AUP form to the Chief Information Security Officer (CISO). A copy of the form is appended to this Policy and is also available online. In submitting the AUP Acknowledgement Form, 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 Touro. Should there be questions as to which policy applies; requests for clarifications should be addressed, in writing, to the CISO at CISO@touro.edu.

Touro-provided email is considered the primary official communication mechanism recognized by Touro for communication with the Touro Community.

IMPORTANT DISCLAIMER

This policy does not form a contract. Touro College 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 Touro College other than its obligations under the law. As with all Touro College 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 Touro College'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 Touro College's main campus.

[1] This policy is not intended as an etiquette guide; however, proper use of email can be derived from various online sites simply by doing a search using Google on the "email use guidelines" phrase.

ACCEPTABLE USE POLICY

PURPOSE 3

AUTHORIZATION 3

PRIVACY 3

ACCEPTABLE USE 4

UNACCEPTABLE USE 4

SECURITY BREACHES 6

MEDIA PERMISSION 7

WARNING NOTICE

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

Any member of the Touro Community found to have violated this Policy may be subject to disciplinary action, according to the applicable Touro Handbook.

EXCEPTIONS TO POLICY

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.

PURPOSE

Touro 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 Touro 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 the Touro's reputation.

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

AUTHORIZATION

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

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

Touro sees privacy, not regulated by law (such as Family Educational Rights and Privacy Act (FERPA) or Health Insurance Portability and Accountability Act (HIPAA)), is 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 Touro Community leaves Touro, files left behind on any computer system owned by Touro, including servers, and electronic mail files, will be kept for a period consistent with record retention policies of Touro and then destroyed. Records maintained on Touro's systems are the sole and exclusive property of Touro College and no privacy right attaches to such records 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 Touro 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 Touro.
- Conventional norms of behavior apply to IT-based media, just as they would apply to more traditional media. Within Touro, this would mean that the tradition of academic freedom will always be respected. Touro, 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.
- All users of Touro 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 Touro 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 Touro may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. The use of Touro 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 Touro is unacceptable. **Unacceptable** use of Touro IT resources may be summarized as:

- Distributing materials which are offensive, obscene, defamatory or abusive. Such material may be illegal and violate Touro policies on abuse. Users of Touro computer systems must be familiar with, and comply with, Touro 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.
- 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 using programs or sending emails that solicit another person's account and password, are unacceptable. Receipt of unsolicited "spam email" should be sent to the CISO@touro.edu for follow up, wherever practical.

- Attempting to break into, gain access to, or damage computer systems or data of Touro computers or any other computers for which the individual is not authorized, or attempting to facilitate actions to accomplish same, is unacceptable.
- Connecting an unauthorized device to Touro'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, is unacceptable.
- 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, is unacceptable.
- Users should not provide any services to others via remote access. The installed machine on each network socket must be a workstation only and not provide any server-based services, including, but not limited to, Web, FTP, Streaming Media server, peer-to-peer facilities, or email services.
- No Touro system or network may be used for any purpose or in a manner that violates Touro policies or federal, state or local law.
- Use of Touro systems or networks for commercial purposes is prohibited.
- Users are not to reconfigure or otherwise adjust any settings on any Touro shared computer, device, technology resource, software and/or hardware without explicit permission from the VP for Technology at Touro or designated staff.
- Users are not permitted to remove any equipment from Touro without explicit permission of Touro Administrative Management.
- It is unacceptable to send student (FERPA-governed) or patient (HIPAA-governed) data via email or to store this type of confidential data on any portable device or virtual space outside of Touro's administrative control in an unencrypted state.
- With Respect to Restricted and Confidential Touro Data:
    - Access is allowed solely to members of the Touro Community to perform 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.
    - Members of the Touro 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. 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.
    - Members of the Touro Community should not make or permit unauthorized use of any restricted or confidential data in any of the College's computer systems or other records. 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.
    - Members of the Touro Community should not enter, change, delete or add data to any computer system or files outside of the scope 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.

- Members of the Touro Community should not include or cause to be included in any record or report, a false, inaccurate or misleading entry known to the user as such. 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.
- Members of the Touro Community should not alter or delete or cause to be altered or deleted from any records, report or information system, a true and correct entry. 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.
- Members of the Touro Community should not release restricted or confidential data other than what is required in completion of job responsibilities which is consistent with this Policy. 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.
- Members of the Touro Community should not 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 Touro's policy that all suspicious activity be immediately reported, especially if the individual has violated this Policy. Additionally, given the potential harm that the College 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:

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

- Non Faculty should report 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 Touro 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.

- Touro 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 Touro Counsel and Senior Management in reporting computer breaches to law enforcement authorities.

MEDIA PERMISSION

User grants the right and permission, without reservation, to Touro College, and those authorized by Touro College, to photograph and/or videotape user and further to display, use and/or otherwise utilize, in original or modified form, user's face, likeness, name, information, voice, and appearance forever and throughout the world, in all media, whether now known or hereafter devised, throughout the universe in perpetuity (including, without limitation, in online webcasts, television, motion pictures, films, newspapers, publications or use by third parties) and in all forms including, without limitation, digitized images, whether for advertising, publicity, or promotional purposes, including, without limitation, for the promotion, public education, and/or fundraising activities of Touro College, without compensation, reservation or limitation. Touro College is, however, under no obligation to exercise any rights granted herein. User releases Touro College, its officers, directors, agents, employees, independent contractors, licensees and assignees from all claims that user now has or in the future may have, relating, thereto. User agrees that Touro College, or its grantees or assignees, will be the sole owner of all tangible and intangible rights in the abovementioned photographs and recordings, with full power of disposition. If potential users or user wishes to opt out of this media permission only please send an electronic mail to barbara.franklin@touro.edu. You cannot opt out of the remainder of this Policy and emailing Touro College will not relieve you of your obligations hereunder.