10-01.02 – Acceptable Use Policy

I. Policy Statement:

Towson University (“University”) students, faculty, and staff have responsibilities and obligations regarding access to and use of University information technology ("IT") resources. Activities outsourced to off-campus entities should comply with similar security requirements as in-house activities.

Access to and use of IT Resources owned and operated by the University is granted subject to University policies, and local, state, and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals’ rights to privacy and to freedom from intimidation and harassment.

Towson University's IT Resources are the property of the University and usage is subject to monitoring, without notice, of all activities as necessary for system maintenance, information security, as required by law and/or to support research of law violations or institutional policy. The purpose of this policy is to outline the acceptable use of IT Resources at the University.

II. Definitions:

A. “IT Resources” All University-owned, operated, or managed computers, applications software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; classroom technologies; communication services and devices. Cloud-Based Systems, including University and Third-Party E-mail Systems, voice mail, modems, multimedia equipment, wired networks, and wireless networks. The components may be stand-alone or networked and may be single-user or multi-user systems.

B. "Electronic Communication" Any means of transmitting and receiving messages over electronic media including, but not limited to, a smartphone, cell phone, telephone, fax, tablet or computer.

C. "Third-party E-mail Systems" E-mail services provided on behalf of the University through third party service providers (e.g., Google Mail, Office 365, or other similar type services).

D. "University E-mail System" E-mail services provided by the University through the Office of Technology Services.

E. "Cyberbullying" Is a form of harassment directed towards another person(s) or organization directly or indirectly via IT Resources that is so severe, pervasive, or persistent that it interferes with or limits a person's ability to participate in, or benefit from, the services, activities, or opportunities offered by the University.

F. "Cloud-Based Systems" Include IT Resources that are hosted by third-parties on behalf of the University and include, but not limited to the following use-cases: Infrastructure-as-a-service, Platform-as-a-Service, and Software-as-a-Service.

I. Responsible Executive and Office:

Responsible Executive:
Vice President for Administration & Finance and Chief Fiscal Officer

Responsible Office:

Office of Technology Services

II. Entities Affected by this Policy:

All divisions, colleges, departments and operating units; University faculty, staff, and students and any other persons using IT Resources.

III. Procedures:

A. General Use

The University's IT Resources are the Property of the University. Access to the University's IT resources is a privilege and must be treated as such by all users. Users are responsible for their actions and are required to:

1. Protect their user IDs and system from unauthorized use. Users are responsible for all activities on their user IDs or that originate from their system.
2. Access only information that is their own, that is publicly available, or to which they have been given authorized access.
3. Act responsibly and abide by all applicable laws, licenses, copyrights, contracts and other limitations on access to and/or use of restricted or propriety information. Use copyrighted software only in compliance with vendor license agreements.
4. Be considerate in their use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or excessively and/or wastefully using computer resources, such as disk space, printer paper, or other resources.
5. Protect sensitive non-public information contained on mobile and desktop devices from unauthorized access.
6. Attend annual information security awareness training as provided by the Office of Technology Services.
7. Use hardware and software that is appropriately licensed and in accordance with licensing agreements.
8. Understand that system administrators may examine electronic files, electronic mail and printer listings for the purpose of diagnosing and correcting problems with the system.
9. Ensure computing device(s) have the latest security software (anti-virus, personal firewalls, etc.) and patches installed and up to date at all times, except for those computers managed by OTS, such as faculty/staff computers.
10. Ensure physical security (e.g., cable locks, locked rooms, etc.) of University IT Resources.
11. Complete all required security awareness training activities (e.g., annual security awareness training for faculty and staff, etc.).

B. Other Responsibilities

Each college, department and administrative unit is responsible for security on its computer systems in accordance with the University's policies and standards and may apply more stringent security standards than those detailed here while connected to the University's information technology resources. Local computer system administrators are responsible for ensuring that appropriate security is enabled and enforced in order to protect the University's information technology

resources. Local computer system administrators, which are sometimes appointed at a department's discretion, must make every effort to remain familiar with the changing security technology that relates to their computer systems and continually analyze technical vulnerabilities and their resulting security implications.

C. Unacceptable uses include, but are not limited to, the following:

1. Using another person's user ID, or password.

2. Using computer programs to decode passwords or access-controlled information.

3. Misrepresenting your identity or affiliation in the use of information technology resources. This includes misrepresenting or implying that the content of a personal homepage constitutes the views or policies of the University.

4. Attempting to alter system, hardware, software or account configurations.

5. Launching computer-based attacks against other users, computer systems, or networks.

6. Connecting devices (switches, routers, wireless access points, etc.) to the network that are not approved by the Office of Technology Services.

7. Accessing or monitoring another individual's accounts, files, software, electronic mail or computer resources without the permission of the owner.

8. Misusing the University's computing resources so as to reduce their efficiency or to affect access to the detriment of other users.

9. Using IT Resources to engage in cyberbullying or harassment, or to transmit obscene or fraudulent messages.

10. Widespread dissemination of unsolicited or unauthorized communication messages such as email chain letters or broadcasting messages to individuals or lists of users, or producing any communication which interferes with the work of others.

11. Knowingly breaching or attempting to breach computer security systems, whether with or without malicious intent.

12. Engaging in any activity that might be harmful to systems or to any stored information such as creating or propagating viruses, worms, Trojan Horses, or other rogue programs; disrupting services or damaging files.

13. Violating copyright and/or software license agreements. Web pages, electronic mail and electronic files may not contain copyright material without the approval from the owner of the copyright.

14. Using IT Resources for commercial or profit-making, or mining of electronic currency purposes without written authorization from the University.

15. Disobeying lab, system, or University policies, procedures, or protocol.

16. Installing or operating computer games on University-owned computers for purposes other than academic instruction.

17. Downloading or posting to University computers, or transporting across University networks, material that is illegal, proprietary, in violation of University contractual agreements, or in violation of University policy.

18. Using IT Resources in violation of any local, state of federal laws.

D. Access and Disclosure

1. The University reserves the right to limit, restrict or remove access to its IT Resources when policies or laws are violated and to use appropriate means to safeguard its

resources, preserve network/system integrity, and ensure continued service at all times.

2. The University does not routinely or randomly inspect, monitor, or disclose information about individuals' use of the University's IT Resources without the user's consent. Notwithstanding, users should have no expectation of privacy in their use of the University's IT Resources, and the University shall have the right, in its direction, to access, retrieve, inspect, monitor, and disclose users' accounts and use of IT Resources:

1. a. to maintain IT system integrity and security;
   b. to protect health and safety;
   c. to prevent interference with the academic mission of the University;
   d. when there is reason to believe that an individual is violating the law or a University policy;
   e. to perform required internal investigations; and
   f. as otherwise required by law or applicable policy.

3. When monitoring of specific restricted activity of faculty or staff accounts is required, the CIO, Director of Information Security or designee will consult with an academic or administrative unit's Dean or Vice President, or designee, prior to monitoring as appropriate based on the reason for the monitoring and/or investigation. If the matter directly involves a Dean or Vice President, the President will be consulted.

4. All investigations, security monitoring related to confidential data or restricted data will be treated as confidential. The University will not disclose privileged or confidential communications from legal clients, attorney work product, student information, employee information, or medical or health care record information unless permitted by law, authorized by the client or patient, or approved by the school, unit or Affiliate that maintains the information.

E. Reporting Violations

All suspected violations must be reported immediately to the proper authorities. For alleged student violations, contact the Office of Student Conduct and Civility Education. For faculty and staff, contact your immediate supervisor. For all others, contact the Office of Technology Services Information Security.

Additionally, violations can be reported to SpeakTU at https://www.towson.edu/counsel/ethics-compliance-violations.html (https://www.towson.edu/counsel/ethics-compliance-violations.html) a 24-hour / 7 day a week hotline.

F. Enforcement

The University considers any violation of acceptable use policies to be a serious offense and reserves the right to copy and examine any files or information residing on University systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations.

Violations may result in disciplinary action in accordance with applicable University policies, handbooks, codes and procedures. Offenders also may be prosecuted under applicable local, State and Federal laws.

Violations may result in revocation or restriction of computer and information resource privileges such as loss of access or disablement of user ids.

The Director of Information Security Officer reserves the right to audit computer and network systems on a periodic basis to ensure compliance with this policy.

Related Policies:

TU Policy 10-5.00-Data Governance Policy (https://www.towson.edu/about/administration/policies/10-05-00-data-goverance-policy.html)
TU Policy 10-01.01 – Information Technology Security Policy (https://www.towson.edu/about/administration/policies/10-01-01-information-technology-security-policy.html)
TU Policy 07-01.00, et seq. – Human Resources Policies (https://www.towson.edu/about/administration/policies/hr.html)
Code of Student Conduct (https://www.towson.edu/studentaffairs/policies/documents/code_of_student_conduct.pdf)
Guidelines for Responsible Computing (https://www.towson.edu/technology/about/policies/computing.html)
Data Governance Roles and Responsibilities Guidelines (https://www.towson.edu/technology/about/policies/index.html)

Approval Date: 10/09/2010

Effective Date: 10/09/2010

Amended Date: 03/10/2021

Approved By: President's Council 03/10/2021

Signed By: President's Council

HOW TO REQUEST THE POLICY PDF

This online version of the policy may include updated links and names of departments. To request a PDF of the original, signed version of this policy, email the Office of the General Counsel, generalcounsel@towson.edu.