University Policies and Procedures

10-01.02 – ACCEPTABLE USE POLICY

I. Policy Statement: Each member of the Towson University ("University") community has responsibilities and obligations regarding access to University computing and information resources. Activities outsourced to off-campus entities should comply with similar security requirements as in-house activities.

Access to computing and information 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.

II. Reason for Policy: The purpose of this policy is to outline the acceptable use of computer systems at the University.

III. Definitions:

A. Information Resource: Includes all University-owned computers, applications software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; classroom technologies; communication services and devices, including electronic mail, voice mail, modems, and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems.

IV. Responsible Executive and Office:
Responsible Executive: Vice President for Administration & Finance and Chief Financial Officer

Responsible Office: Office of Technology Services

V. Entities Affected by this Policy: All divisions, colleges, departments and operating units; University faculty, staff, and students and any other persons using University information resources.

VI. Procedures:

A. General

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

1. Use resources only for authorized purposes.

2. 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.

3. Access only information that is their own, that is publicly available, or to which they have been given authorized access.

4. Abide by all applicable 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.

5. 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.

6. Protect sensitive non-public information contained on mobile and desktop devices from unauthorized access.

7. Attend annual information security awareness training as provided by the Office of Technology Services.

8. Act responsibly so as to ensure the integrity and lawful use of computing and information resources.

9. Respect the rights of others and not threaten, harass, intimidate or engage in unlawful activity.

10. Understand that system administrators may examine electronic files, electronic mail and printer listings for the purpose of diagnosing and correcting problems with the system.

11. Understand the University has the right to restrict or rescind computing privileges in accordance with this and other applicable University policies

when the user has exhibited inappropriate behavior in the use of computer facilities or information resources.

12. Web pages, electronic mail and electronic files may not contain copyright material without the approval from the owner of the copyright.

13. 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.

14. Ensure TU-owned personal computer hardware has been secured (e.g. cable locks, etc).

B. Other Responsibilities

Each college, department and administrative unit is responsible for security on its computer systems 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. Producing chain letters or broadcasting messages to individuals or lists of users, or producing any communication which interferes with the work of others.

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

11. 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.

12. Violating copyright and/or software license agreements.

13. Using computing resources to threaten or harass others or transmitting obscene or fraudulent messages.

14. Using computing resources for commercial or profit-making 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. Violating local, state or federal laws.

D. 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 Officer.

E. 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. Revocation or restriction of computer privileges is also possible. Offenders also may be prosecuted under applicable local, State and Federal laws. The Information Security Officer reserves the right to audit computer and network systems on a periodic basis to ensure compliance with this policy.

Related Policies: None.

Approval Date: 10/09/2010

Effective Date: 10/09/2010

Approved by: President's Council 09/30/2010