University Policies and Procedures

10-01.01 – INFORMATION TECHNOLOGY SECURITY POLICY

I. Policy Statement:

Each member of the campus community is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

II. Reason for Policy:

The purpose of this policy is to establish a framework for ensuring that Towson University’s (the “University”) information technology (IT) resources are managed securely. These resources include information, information systems, computing platforms, and networks. It also ensures that the University complies with state laws and regulations regarding the use of and security of information resources.

III. Definitions:

A. Information Technology (IT) Resources - IT Resources 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.

B. Critical Information System – Computer system that stores and processes information that is vital to the University business.

C. Sensitive Information – Data in electronic or paper form that contains personal data about a person (e.g. social security number, credit card number, etc.).

IV. Responsible Executive and Office:

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

Responsible Office: Office of Technology Services

10-01.01 - 1
V. **Entities Affected by this Policy:** All divisions, colleges, departments and operating units and University faculty, staff, students, non-employees and guests of the University.

VI. **Procedures:**

A. **Risk Management**

The Office of Technology Services (OTS) will establish a risk management program that includes identifying critical information systems and performing a risk self assessment annually. Departments are required to identify critical information systems in their control. Departments will classify and secure information according to its sensitivity to meet federal and state laws. Departments will devise local policies and procedures for protecting sensitive information in their care. OTS will establish a program to identify and resolve critical vulnerabilities in all campus information systems. Any critical vulnerability found must be resolved in a timely manner. Departments processing, storing and transmitting credit card information will be required to complete a security questionnaire annually.

B. **Access Controls**

No one may access confidential records unless specifically authorized to do so. Even authorized individuals may use confidential records only for authorized purposes. Each authorized user (specific individual) is assigned a unique password that is to be protected by that individual and not shared with others, difficult to crack, changed on a regular basis, and deleted when no longer authorized. Users are responsible for creating and protecting passwords that grant them access to resources. Passwords must adhere to the OTS Password Guidelines located at: [http://towson.edu/technology/about/policies/password.html](http://towson.edu/technology/about/policies/password.html).

OTS and Departments shall maintain and periodically review user access privileges, and revise them as required by changes in job function, transfers, and affiliation with the University.

Individuals must take care to ensure that their systems are configured so as to prevent unauthorized access. When remote access is allowed, special care shall be taken to select safe implementation options and ensure that passwords and other access controls are respected. Remote access to the campus network shall use secure communications where possible.

OTS will ensure that controls are in place to avoid unauthorized intrusion of systems and networks and to detect efforts at such intrusion.

C. **Physical Security**
Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where server devices are located, to simple measures taken to protect a user’s display screen. Users shall provide physical security for their information technology devices. Access to data centers and secure areas should be restricted to individuals with job responsibilities requiring them access. Authorized visitors shall be supervised. Locks, cameras, alarms, etc. must be installed in technology centers and closets to discourage and respond to unauthorized access.

D. Computer Security

All microcomputers (i.e., workstation, desktop computers, notebook computers, personal digital assistants and any other portable device used for University work or accessing University information that processes/transmits/stores data) must be secured against unauthorized access. The level of controls must be commensurate with the information accessed, stored, or processed on these devices. All microcomputers must be secured using user identification and password. Standard virus protection programs must be installed, updated, and maintained on all microcomputers and servers connected to the campus computer network.

E. Network Security

OTS will maintain network security through a combination of technologies including, but not limited to, switched networks, strong authentication, encryption, intrusion detection/prevention systems, and firewalls where appropriate. OTS will periodically check the network and network servers for vulnerabilities, using software tools designed for this purpose.

F. Disaster Recovery and Business Continuity

OTS will implement, and regularly update, an IT disaster recovery process to counteract interruptions to normal University activity and to protect critical processes from the effects of failures or damage to vital services or facilities. Data and software essential to the continued operation of critical University functions will be backed up by OTS. The security controls over the backup resources will be as stringent as the protection required of the primary resources. Backup of data and software stored on centrally administered computer systems is the responsibility of OTS. Colleges and departments administering servers are responsible for establishing regular schedules for making backup copies of all mission-critical data and software resident on their servers and for ensuring that the backups are stored in a safe location. Each Department is responsible for developing, testing and maintaining a business continuity plan consistent with University standards.
G. Information Security Awareness program

The Information Security Officer (ISO) shall implement a security awareness program and shall provide information and further training in information security matters to answer particular requirements. It is recommended that all members of the campus community receive some form of annual information security awareness education.

H. Incident handling and reporting

Users must report suspected or known compromises of information resources, including contamination of resources by computer viruses, to their Managers and/or the Information Security Officer in OTS. Users shall cooperate with any investigation. Incidents will be treated as confidential unless there is a need to release specific information.

I. Enforcement

Failure to comply with this policy may result in immediate deactivation of the user’s account or denial of network access to the user’s device. Disciplinary action may also be taken, including but not limited to termination of employment. Students may be subject to the Towson University Code of Student Conduct, which could result in judicial sanctions, including but not limited to, suspension or expulsion from the University. The University may routinely monitor network traffic to assure the continued integrity and security of University resources in accordance with applicable policies and laws.

Related Policies:

USM Policy X-1.00 Policy on USM Information Technology

TU Policy 10-03.00, Electronic Mail Policy

See also:

Policies, including Functional Compatibility with the State

Information Technology Plan

Guidelines for Responsible Computing

OTS Password Management Standards

OTS Desktop Security Standard
OTS Server Security Standard

Approval Date: 05/21/2009

Effective Date: 05/21/2009

Approved by: President’s Council 05/18/2009