The University of North Texas at Dallas Policy Manual	Chapter 14.000
14.008 Acceptable Use	**Information Technology**

Policy Statement. It is the policy of the University of North Texas at Dallas to manage the University's information resources as strategic assets of the State of Texas. The University provides each of its authorized users with one or more accounts that permit use of the University's information resources for the purpose of accomplishing tasks related to the University's mission. This policy is established to achieve the following:

i. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

ii. To establish prudent and acceptable practices regarding the use of information resources; and,

iii. To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Application of Policy. This policy applies to the total University.

Definitions.

1. Information Resources. "Information Resources" mean the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data and administered both centrally and within individual departments, on-campus and remotely, on a mainframe and network servers, and for use by single and multiple users.

2. University Users. "University Users" mean all faculty, staff, students, contractors, volunteers, and individuals that maintain a business relationship with the University and are granted access privileges to any of the University's information resources. Information resources may also be included in this category.

Procedures and Responsibilities.

1. **General Provisions.** This policy applies to all University information resources.

    1.01. Freedom of Expression. Use of information resources will be consistent with the University policies regarding harassment, plagiarism, and unethical conduct.

1.02. Intellectual Property. Laws related to the protection of intellectual property extend to the electronic environment. Users should assume that works communicated through the computer network are subject to all federal and state laws, regulations, and University policies regarding copyright, trademark, and intellectual property unless specifically stated otherwise.

1.03. Privacy. Privacy will be extended to university users while using information resources to the extent set forth in the University Information Resources Privacy Policy. Use of the University's information resources and transmission of content via such resources may be subject to:

a. Review or disclosure in accordance with the Texas Public Information Act and other laws;
b. Administrative review of information resource use for security purposes or in regard to a policy or legal compliance concern;
c. Information resources maintenance;
d. Audits and as otherwise required to protect the reasonable interests of the University and other users of the information resources.

2. **Responsibilities of University Users**. All university users are responsible for managing their use of information resources and are accountable for their actions relating to information resource security.

2.01. University users must report any weaknesses in the University's computer security, any incidents of possible misuse or violation of this policy to their supervisor, department head, or Director of Information Technology or designee.

2.02. University users must not attempt to access any data or programs contained on the university systems for which they do not have authorization or explicit consent.

2.03. University users must not share their University account(s), passwords, personal identification numbers (PIN), security tokens (i.e., Smartcard), or similar information or devices used for identification and authorization purposes.

2.04. University users must not purposely engage in activity that may: degrade the performance of information resources; deprive an authorized university user access to a University resource; obtain extra resources beyond those allocated; circumvent university computer security measures.

2.05. University users must not intentionally access, create, store or transmit material which violates University policies regarding harassment and unethical conduct. In the course of academic research, University users must obtain the explicit approval of a relevant University official to use information resources in a manner that may otherwise violate such university policy.

2.06. University users must not otherwise engage in acts against the mission of the University as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

2.07. Users are responsible in adhering to relevant information resources policies.

Responsible Party: All University Users

3. **Incidental Use.** As a convenience to the University user community, incidental use of information resources is permitted. The following restrictions apply:

3.01. Incidental personal use of resources such as electronic mail, Internet access, fax machines, printers, and copiers is restricted to university-approved users; it does not extend to family members or other acquaintances;

3.02. Incidental use must not result in direct costs to the University;

3.03. Incidental use must not interfere with the normal performance of an employee's work duties;

3.04. No files or documents may be sent or received that may cause legal action against the University or impair the University's mission;

3.05. Storage of personal email messages, voice messages, files and documents within the University's information resources must be nominal; and

3.06. All messages, files and documents, including personal messages, files and documents, located on University information resources are owned by the University, may be subject to open records requests, and may be accessed in accordance with this policy.

Responsible Party: All University Users

4. **Responsibilities of Deans, Department Heads, and Supervisors**.

4.01. Ensure that employees within a department receive opportunities to attend training courses that help them to comply with this policy and other applicable University policies.

4.02. Promptly inform appropriate system administrators when employees have been terminated so, that the terminated employee's access to University information resources may be disabled.

4.03. Promptly report ongoing or serious problems regarding information resource use to the Director of Information Technology.

Responsible Party: Deans, Department Heads, and Supervisors

5. **Auditor Access**. There will be occasions when auditors require access to University information resources and data files. The access will be permitted in accordance with the following guidelines:

5.01. Internal auditors shall be allowed access to all University activities, records, property, and employees in the performance of their duties. Internal auditors shall notify the Director of Information Technology and the Office of the General Counsel prior to accessing individual data files.

5.02. Upon notification to the Office of General Counsel, State and federal auditors will be granted access to University information resources and data files on an as needed basis.

Responsible Party: Director of Information Technology/Office of the General Counsel

6. **Prohibitive Actions.** The following actions constitute misuse of the University's information resources and are strictly prohibited for all university users:

6.01. University information resources are not to be used in support of or for criminal and illegal activities, such as unauthorized access, intentional corruption or misuse of information resources, theft, obscenity, and child pornography.

6.02. Failure to comply with laws, policies, procedures, license agreements, and

contracts that pertain to and limit the use of the University's information resources.

6.03. Abuse of information resources including, but not limited to, any act which endangers or damages specific computer software, hardware, program, network or the system as a whole, whether located on campus or elsewhere on the Internet; creating or purposefully allowing a computer malfunction or interruption of operation; intentionally injecting a computer virus on the computer system; sending a message with the intent to disrupt university operations or the operations of outside entities; and, failure to adhere to time limitations which apply at particular computer facilities on campus.

6.04. Use of the University's information resources for personal financial or commercial gain, commercial or personal advertisement, solicitations, promotions, or employee's transmission of political material is prohibited.

6.05. Failure to protect a password or account from unauthorized use.

6.06. Permitting someone to use your computer account, or using someone else's computer account.

6.07. Unauthorized use, access, reading, or misuse of any electronic file, program, network, or the system.

6.08. Unauthorized use, access, duplication, disclosure, alteration, damage, misuse, or destruction of data contained on any electronic file, program, network, or University hardware or software.

6.09. Unauthorized duplication and distribution of commercial software and other copyrighted digital materials.

6.10. Attempting to circumventor assisting or requesting the circumvention of any security measure or administrative access control that pertains to University information resources.

6.11. Use of the university computer system in a manner that violates other university policies pertaining to racial, ethnic, religious, sexual or other forms of harassment.

Responsible Party: All University Users

7. **Potential Liability for Failure to Adhere to Policy.** All university users that fail to adhere to this and other information resources policies may have their information resources account(s) cancelled. Additionally the users may be suspended, dismissed or other disciplinary actions taken by the University, as well as referral to law enforcement agencies.

Responsible Party: All University Users

References and Cross-references.

Texas Government Code § 2054 – Information Resources

Texas Administrative Code, Chapter 202, Subchapter C and Department of Information Resources, Policy and Standards for Protecting Information Resources for Texas

University of North Texas at Dallas Electronic Communications Policy; Internet Use Policy; Information Services Privacy Policy; Portable Computing Policy; Software Licensing Policy; Password Protection Policy; Network Access Policy; and Information Resources Security Policy

Approved: 8/30/2010

Effective: 8/30/2010

Revised: