1. Title

Information Resources Acceptable Use and Security Policy

2. Policy

Sec. 1 Purpose. The subsections of this document comprise The University of Texas System Administration Information Resources Acceptable Use and Security Policy. This policy is established to achieve the following:

1.1 to establish prudent and acceptable practices regarding the use and safeguarding of Information Resources;

1.2 to protect the privacy of individuals for whom personally identifiable information is held including protected health information and education records;

1.3 to educate individuals who may use Information Resources with respect to their responsibilities associated with such use;

1.4 to ensure compliance with applicable statutes, regulations, and mandates regarding the management of Information Resources; and

1.5 to gain a signed annual acknowledgement of this policy from every individual granted access to U. T. System Administration Information Resources.

Note: A companion document to this policy, the U. T. System Administration Information Resources Standards of Operation Manual, details security practices and requirements relating to each policy topic and is incorporated by reference into this policy. These two documents comprise the policy and procedures foundation for the U. T. System Administration computer security program.

Sec. 2 Protection of Assets. The assets of the U. T. System Administration must be available and protected commensurate with their value and must be administered in conformance with federal and State law and the Board of Regents' *Rules and Regulations*. Measures shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. As stated in Title 1 *Texas Administrative Code* 202.20 (1), it is the policy of the State of Texas that Information Resources residing in the various agencies of State government are strategic and

vital assets belonging to the people of Texas. The formal acknowledgment of the Acceptable Use and Security Policy serves as a compliance and enforcement tool.

Sec. 3 Information Resources Acceptable and Secure Use.

3.1 Individual Responsibility. All individuals granted access to technology resources of U. T. System Administration must acknowledge the rules of use of these resources annually. Each individual is responsible for exercising good judgment regarding the reasonableness and security of his/her behavior and use of Information Resources.

3.2 Incidental Personal Use. As a convenience to individuals, limited incidental personal use of Information Resources is permitted. Incidental use of Information Resources must not result in direct cost to the U. T. System Administration or expose U. T. System Administration to unnecessary risks.

Sec. 4 Disciplinary Actions.

4.1 Monitoring Authority. Pursuant to Title 1 *Texas Administrative Code* Section 202 and to ensure compliance with this policy and State laws and regulations related to the use and security of Information Resources, U. T. System Administration has the authority and responsibility to monitor Information Resources. If there is a reasonable basis to believe that this policy or State laws or regulations regarding the use and security of Information Resources have been violated, the contents of user files may be accessed for purposes of investigation with the written approval of a U. T. System Administration executive officer.

4.2 Types of Disciplinary Action. Violation of this policy may result in disciplinary action for employees, including but not limited to, termination. For contractors and consultants this may include a termination of the work engagement. For interns and volunteers, this may include dismissal. Any student who violates this policy will be referred to student judicial services at the student's home campus. Additionally, individuals are subject to possible civil and criminal prosecution.

Sec. 5 All Other Procedures. For all other procedures and mechanisms outlined in this policy and UTS165, consult the Information Resources Standards of Operation Manual. Compliance with these procedures will be enforced as outlined in the Disciplinary Actions section of this policy.

3. Definitions

Backup - copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

Custodian - guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. The Office of Technology and Information Services (OTIS) acts as custodian of network resources at U. T. System Administration.

Change Management - the process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

Change -

- any implementation of new functionality;
- any interruption of service;
- any repair of existing functionality; or
- any removal of existing functionality.

Confidential Data - data that is exempt from disclosure under the provisions of the Public Information Act or other applicable State and federal laws.

Electronic Mail (Email) - any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Electronic Mail System - any computer software application that allows electronic mail to be communicated from one computing system to another.

Email - abbreviation for electronic mail.

Information Resources (IR) - any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, handheld computers, personal digital assistants (PDAs), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Facilities - any location that houses Information Resource equipment (includes servers, hubs, switches, and routers). Facilities are usually dedicated rooms or mechanical/wiring closets in the buildings.

Integrity - the accuracy and completeness of information and assets and the authenticity of transactions.

Internet - a global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

Local Area Network (LAN) - a data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Office of Technology and Information Services (OTIS) - the name of the U. T. System Administration department responsible for computers, networking, and data management.

Owner - the manager or agent responsible for the function that is supported by the resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Password - a string of characters used to verify or "authenticate" a person's identity.

Portable Computing Devices - any easily portable device that is capable of receiving and/or transmitting data. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell phones.

Strong Passwords - a strong password is constructed so that another user or a "hacker" program cannot easily guess it. It is typically a minimum number of positions in length and contains a combination of alphabetic, numeric, or special characters.

Scheduled Change - formal notification received, reviewed, and approved through the review process in advance of a change being made.

Sensitive Data - Digital Data maintained by an entity that requires higher than normal security measures to protect it from unauthorized access, modification, or deletion. Sensitive Data may be either public or confidential and is defined by

each entity based on compliance with applicable federal or State law or on the demonstrated need to (a) document the integrity of that Digital Data (i.e., that the Data had not been altered by either intent or accident), (b) restrict and document individuals with access to that Digital Data, and (c) ensure appropriate backup and retention of that Digital Data. These would most frequently be required by

- federal agencies (e.g., Food and Drug Administration);
- State agencies (e.g., data defined as High-Risk Information Resources by 1 *Texas Administrative Code* 202.72);
- employee benefit providers;
- Office of General Counsel or Entity Office of Legal Affairs (i.e., data subject to or involved in litigation or confidentiality agreements);
- Intellectual Property and/or Technology Transfer requirements; or
- federal regulations (e.g., Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act, Biodefense, Homeland Security, Department of Defense (DOD), etc.)

Server - a computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Trojan Horse - a destructive program, usually a virus or worm, that is hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by email or on a diskette or CD, often from another unknowing victim, or may be urged to download a file from a website or bulletin board.

User - an individual, automated application, or process that is authorized by the owner to access the resource, in accordance with the owner's procedures and rules. User includes employees, faculty, contractors, and others and has the responsibility to (a) use the resource only for the purpose specified by the owner, (b) comply with controls established by the owner, and (c) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized by the owner of the information to read, enter, or update that information. The user is the single most effective control for providing adequate security.

Vendor - someone outside of U. T. System Administration who exchanges goods or services for money.

Virus - a program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus

infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

Web Page - a document on the World Wide Web. Every web page is identified by a unique URL (Uniform Resource Locator).

Web Server - a location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A website always includes a home page and may contain additional documents or pages.

World Wide Web - also referred as the Web is a system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language), which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.

Worm - a program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network, using otherwise-unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors.

4. Relevant Federal and State Statutes

Title 1 *Texas Administrative Code* Part 10, Chapter 202, Subchapter C

5. Relevant System Policies, Procedures, and Forms

U. T. System Administration Information Resources Standards of Operation Manual

UTS165, *UT System Information Resources Use and Security Policy*

Information Resources Acceptable Use Policy Agreement Form

6. System Administration Office(s) Responsible for Policy

Office of General Counsel
Office of Technology and Information Services

7. Dates Approved or Amended

February 1, 2006
July 8, 2009
August 4, 2011

8. Contact Information

Questions or comments about this policy should be directed to:

- bor@utsystem.edu