



**SUB-TOPIC**

**Information Resources Use and Security Policy**

## 1. Overview

The assets of The University of Texas at Dallas (“UTD”) must be available, protected commensurate with their value, and must be administered in conformance with federal and state law and The University of Texas System 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 202.2 (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 subsections of this document comprise The University of Texas at Dallas Information Resources Use and Security Policy. This policy is established to achieve the following:

- To establish prudent and acceptable practices regarding the use and safeguarding of Information Resources.
- To protect the privacy of individuals for whom we hold personally identifiable information including protected health information and education records.
- To educate individuals who may use Information Resources with respect to their responsibilities associated with such use.
- To ensure compliance with applicable statutes, regulations and mandates regarding the management of Information Resources.

**NOTE:** A companion document to this policy, The University of Texas at Dallas Information Resources Security Operations Manual, details security practices and requirements relating to each policy topic. To facilitate location of related information, the two documents share a common organizational structure and table of contents. These two documents along with The University of Texas at Dallas Information Resources Acceptable Use, E-mail, Server Management and Network Connection Policies comprise the policy and procedures foundation for the UTD Information Security program.

## 2. Audience

The University of Texas at Dallas Information Resources Use and Security Policy applies equally to all individuals that have, or may require, access to UTD Information Resources.

## 3. Information Resources Acceptable Use

Information Resources acceptable use standards are established to protect the valuable Information Resources owned and used by UTD to accomplish the missions and goals of the organization. To ensure all employees can rely on these systems, individuals granted access to any UTD Information Resource must follow the Acceptable Use Policy.



SUB-TOPIC

**Information Resources Use and Security Policy, Continued**

**4. Account Management**

Computer accounts are used to control access to UTD Information Resources and provide accountability for Information Resources usage. Proper management and use of computer accounts are basic requirements for protecting UTD Information Resources. To ensure proper access to Information Resources is granted for the position and duties of the individual, the Office of Information Security is responsible for network account creation and must manage accounts in accordance with The University of Texas at Dallas Information Resources Security Operations Manual and Information Resources Acceptable Use Policy.

**5. Administrative/Special Access**

To ensure all Administrative/Special Access accounts are used only for their intended administrative purpose, all users of such accounts must be made aware of special responsibilities associated with the use of special access privileges and must comply with the Administrative/Special Access section of The University of Texas at Dallas Information Resources Security Operations Manual.

**6. Backup of Network Servers**

Electronic backups are a business requirement to enable the recovery of data and applications in the event of a disaster, system disk drive failures, espionage, data entry errors, human error, or system operations errors. The UTD Information Resources Department requires that owners of servers connected to the UTD network, in accordance with a risk assessment, back up mission critical data and provide a disaster recovery plan.

**7. Change Management**

The Information Resources infrastructure at UTD is constantly changing and evolving to support the missions of the organization and its many departments. To ensure reliable and stable operations the UTD Information Resources Department is required to follow change management procedures to protect and manage UTD Information Resources and establish standards for individuals who manage information systems or applications.

**8. Computer Virus Prevention**

It is the policy of UTD that the network infrastructure and other Information Resources must be continuously protected from threats posed by computer viruses, worms, and other types of hostile computer programs. These threats have the potential of causing significant business disruption and significant cost in terms of failed services, service recovery and costs associated with the potential loss of protected, personally identifiable information. To minimize business disruption and costs associated with hostile computer programs, each computer on the UTD network must run current virus protection software and adhere to any other protective measures required by the Information Resources Information Security Office.



SUB-TOPIC

Information Resources Use and Security Policy, Continued

**9. E-mail**

E-mail, an essential tool for communicating within UTD, must be available at all times and must be used in a manner that does not expose UTD to unnecessary risks. All users who are assigned an E-mail address are required to exercise prudent E-mail use in accordance with The University of Texas at Dallas Information Resources Acceptable Use and E-mail Policies.

**10. Incident Management**

Incidents involving computer security will be reported as required by state law. To ensure that each incident is reported, documented and resolved in a manner that restores operation quickly, the Information Security Office is required to establish and follow incident management procedures.

**11. Incidental Use**

As a convenience to the UTD user community, limited incidental use of Information Resources is permitted. Users are responsible for exercising good judgment regarding the reasonableness of personal use in accordance with The University of Texas at Dallas Information Resources Acceptable Use Policy. Incidental use of Information Resources must not result in direct cost to or expose UTD to unnecessary risks.

**12. Internet Use**

UTD departments use the Internet for publishing information, communicating with the public and business partners, and for delivery of applications in support of UTD and departmental missions. Employees use the Internet to access services, perform research, and communicate with various constituencies. Students use the Internet to further their education and to handle various administrative tasks. There are certain risks associated with the posting or consuming of information on the Internet. To mitigate these risks, UTD network users must adhere to prudent and responsible Internet use practices as outlined in The University of Texas at Dallas Information Resources Acceptable Use Policy.

**13. Information Services (IS) Privacy**

Internal UTD users (including employees, faculty, students, contractors, and others) should have no expectation of privacy with respect to the use of Information Resources:

- Electronic files created, sent, received or stored on computers and other Information Resources owned, leased, administered or otherwise under the custody and control of UTD are not private. They may be accessed as needed for purposes of system administration and maintenance, for resolution of technical problems, for compliance with the Texas Public Information Act, subpoena or court order, to conduct the business of UTD and to perform audits.



SUB-TOPIC

**Information Resources Use and Security Policy, Continued**

- Third parties have entrusted their information to UTD for business purposes. All workers at UTD must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer. Customer account data, protected health information and education record data are confidential and access will be strictly limited based on a business need for access.

**14. Network Access**

UTD's network infrastructure is provided as an essential central resource utility. All network users are required to read and acknowledge The University of Texas at Dallas Information Resources Acceptable Use Policy. To ensure that access to the network does not compromise the operations and reliability of the network or compromise the integrity of information contained within the network, users are required to adhere to The University of Texas at Dallas Network Connection Policy.

**15. Network Configuration**

To ensure reliability of operations, proper accessibility to resources and protection of data confidentiality and integrity, the UTD Information Resources Department is solely responsible for the network infrastructure at UTD and will configure and manage the resource.

**16. Passwords**

Strong passwords shall be used to control access to Information Resources at the University of Texas at Dallas. All passwords must be constructed, implemented and maintained according to the published password guidelines and must be changed at least semi-annually.

**17. Physical Access**

As part of the overall security program at UTD, all Information Resources must be physically protected, based on risk assessment.

**18. Portable Computing and Remote Access**

To preserve the integrity, availability, and confidentiality of UTD's information, all users accessing UTD's infrastructure remotely via computers or other devices must do so in accordance with The University of Texas at Dallas Information Resource Acceptable Use Policy. All users are required to read and acknowledge the policy.

**19. Security Monitoring**

The Information Resources Department is solely charged with securing the network resources at UTD and has the responsibility and authority to monitor network traffic and use of Information Resources to ensure compliance with security practices and controls in place.



SUB-TOPIC

**Information Resources Use and Security Policy, Continued**

**20. Security Training**

The philosophy of protection and specific security instructions must be communicated to computer users. To continuously reinforce and upgrade security awareness and training, the Information Resources Department is charged with providing a combination of general computer security awareness and supported products training.

**21. Server Hardening**

To protect against malicious attack, all servers at UTD will be required to register and comply with The University of Texas at Dallas Server Management Policy.

**22. Software Licensing**

To be in compliance with copyright laws, all software used on UTD computers must be used in accordance with the applicable software license. Unauthorized use of software is regarded as a serious matter subject to disciplinary action and any such use is without the consent of The University of Texas at Dallas.

**23. System Development and Deployment**

To ensure that the protection of Information Resources (including data confidentiality, integrity and accessibility) is considered during the development or purchase of new computer applications:

- The UTD Information Security Office must be consulted in the specification, design, development and deployment of technology initiatives.
- Internal auditors will participate in assuring audit ability during the acquisition and system development process.

Based on risk, outsourced applications and associated data must be properly secured and backed up. Information technology outsourcing contracts must address security, backup and privacy requirements, and should include right-to-audit or other provisions to provide appropriate assurances that applications and data will be adequately protected. Vendors must adhere to all state and federal laws and The University of Texas System Board of Regents' Rules and Regulations pertaining to the protection of Information Resources and privacy of sensitive information.

**24. Vendor Access**

Vendors serve an important function in the support of hardware and software and, in some cases, the operation of computer networks, servers and/or applications. Vendors must comply with all applicable policies, practice standards and agreements, and federal and state laws.



SUB-TOPIC

Information Resources Use and Security Policy, Continued

**25. Disciplinary Actions**

Pursuant to Title 1, Texas Administrative Code 202, and to ensure compliance with this policy and state laws and regulations related to the use and security of Information Resources, UTD 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 UTD executive officer. 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. Additionally, individuals are subject to possible civil and criminal prosecution.

**Definitions**

**Backup:** Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash or other disaster.

**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 is defined as: any implementation of new functionality, any interruption of service, any repair of existing functionality and/or any removal of existing functionality.

**Confidential:** The classification of data of which unauthorized disclosure/use could cause serious damage to an organization or individual.

**Confidential Information:** Information maintained by state agencies and universities that is exempt from disclosure under the provisions of the Texas Open Records Act or other applicable state and federal laws. The controlling factor for confidential information is dissemination.

**E-mail:** Any message, image, form, attachment, data, or other communication sent, received or stored within an electronic mail system.



SUB-TOPIC

**Information Resources Use and Security Policy, Continued**

**Information Resources:** Any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving E-mail, browsing Internet sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), 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 Department:** The name of the UTD department responsible for computers, networking and data management.

**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.

**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 and right to use Information Resources.

**Strong Passwords:** A password 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 and/or special characters.

**Sensitive Information:** Information maintained by state agencies that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. The controlling factor for sensitive information is that of integrity.

**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.



SUB-TOPIC

**Information Resources Use and Security Policy, Continued**

**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. A user has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) 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 UTD 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.

**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.