1. Title Information Resources Use and Security Policy

2. Policy

Sec. 1 Purpose. The purpose of this Policy is to:

(a) establish Standards regarding the use and safeguarding of U. T. System Information Resources;

(b) protect the privacy of individuals by preserving the confidentiality of Personally Identifiable Information entrusted to the U. T. System;

(c) ensure compliance with applicable Policies and State and Federal laws and regulations regarding management of risks to and the security of Information Resources;

(d) appropriately reduce the collection, use, or disclosure of social security numbers contained in any medium, including paper records;

(e) establish accountability;

(f) educate individuals regarding their responsibilities associated with use and management of U. T. System Information Resources; and

g) serve as the foundation for each Institution’s Information Security Program, providing the authority to implement Policies, Standards, and Procedures necessary to implement an effective Information Security Program in compliance with this Policy.

Sec. 2 Policy Statement. Information Resources residing in the Institutions of the University of Texas System are strategic and vital assets belonging to the people of Texas. Access to these resources shall be appropriately managed. It is the policy of The University of Texas System to protect Information Resources based on Risk against accidental or unauthorized access, disclosure, modification, or destruction and assure the availability, confidentiality, and integrity of these resources while avoiding creation of unjustified obstacles to conducting business and achieving the missions of the U. T. System.

Sec. 3 Applicability. This Policy applies to:

(a) all Institutions and organizational units within the U. T. System including the University of Texas Investment Management Company (UTIMCO);

(b) all Information Resources owned, leased, operated, or under the custodial care of any U. T. System Institution, organization, or facility;

(c) all Information Resources owned, leased, operated, or under the custodial care of third-parties operated on behalf of a U. T. System Institution, organization, or facility; and

(d) all individuals accessing, using, holding, or managing University Information Resources on behalf of The University of Texas System.

Sec. 4 Compliance with State Law. Information that is collected pursuant or related to the U. T. System Information Security Program is subject to Section 552.139 of the Texas Government Code and is therefore confidential by law. Accordingly, an Institution may not withhold information or fail to include information required by this Policy and/or Security Standards to be provided to or included in the U. T. System Information Security Program or for administration of program oversight.

Sec 5 Information Security Standards. U. T. System Institutions shall implement and abide by the following Standards:

UTS165 Standard 1.	Information Resources Security Responsibilities and Accountability
UTS165 Standard 2.	Acceptable Use of Information Resources
UTS165 Standard 3.	Information Security Programs
UTS165 Standard 4.	Access Management
UTS165 Standard 5.	Administrative/Special Access Accounts
UTS165 Standard 6.	Backup and Disaster Recovery
UTS165 Standard 7.	Change Management
UTS165 Standard 8.	Malware Prevention
UTS165 Standard 9.	Data Classification
UTS165 Standard 10.	Risk Management
UTS165 Standard 11.	Safeguarding Data
UTS165 Standard 12.	Security Incident Management

UTS165 Standard 13. Use and Protection of Social Security Numbers

UTS165 Standard 14. Information Services (IS) Privacy

UTS165 Standard 15. Passwords

UTS165 Standard 16. Data Center Security

UTS165 Standard 17. Security Monitoring

UTS165 Standard 18. Security Training

UTS165 Standard 19. Server and Device Configuration and Management

UTS165 Standard 20. Software Licensing

UTS165 Standard 21. System Development and Deployment

UTS165 Standard 22. Vendor and Third-Party Controls and Compliance

UTS165 Standard 23. Security Control Exceptions

UTS165 Standard 24. Disciplinary Actions

3. Definitions The following definitions are used within the context of this Policy and all University of Texas System Standards established by this Policy.

Authentication - a process used to verify one's identity.

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

Centralized IT - the institutional information technology services and support organization, reporting to the highest-ranking information technology administrator/officer in the institution, that supports institutional legacy administrative systems or enterprise resource planning (ERP) systems such as student administration (admissions, financial aid, registration, etc.), financial information systems, procurement systems, human resource systems, payroll, research administration (grants and contracts), Network Infrastructure, institutional electronic communications, video, library systems, etc.

Change - any addition or removal of, and any modification or update to an Information Resource.

Change Management - process of controlling the communication, approval, implementation, and documentation of modifications to hardware, software, and

Procedures to ensure that information resources are protected against improper modification before, during, and after system implementation.

Chief Administrative Officer - the highest ranking executive officer at each Institution. For most Institutions, this is the President.

Cloud Computing (Cloud Services) - has the same meaning as "Advanced Internet-based computing service" as defined in *Texas Government Code* 2157.007(a): "a service that provides network access to a shared pool of configurable computing resources on demand, including networks, servers, storage, applications, or related technology services, that may be rapidly provisioned and released by the service provider with minimal effort and interaction. The term does not include telecommunications service or the act of hosting computing resources dedicated to a single purchaser."

Common Use Infrastructure - an IT facility, network, system, or other Information Resource managed, owned or controlled by U. T. System Institutions that provides services to multiple U. T. Institutions under the auspices of the U. T. System. Examples: shared data centers, the U. T. System Network, the U. T. System Identity Management Federation, TexSIS student information system, UTShare HR/Finance, eCRT certification effort reporting system.

Computing Device - any device capable of sending, receiving, or storing Digital Data, including but not limited to: computer servers, workstations, desktop computers, laptop computers, tablet computers, cellular/smart phones, personal digital assistants, USB drives, embedded devices, smart watches and other wearable electronic devices, etc.

Confidential Data - data that is exempt from disclosure under applicable State law, including the Texas Public Information Act, and Federal laws. Data or information meeting these criteria are designated with the classification of "Confidential" within the U. T. System Data Classification Standard.

Controlled Data - one of three data classifications defined within the U. T. System Data Classification Standard. The "Controlled" classification applies to information/data that is not generally created for or made available for public consumption, but that is subject to release to the public through request via the Texas Public Information Act or similar State or Federal law.

Data - elemental units, regardless of form or media, that are combined to create information used to support research, teaching, patient care, and other University business processes. Data may include but are not limited to: written, electronic video, and audio records, photographs, negatives, etc.

Data Center - a facility used to house computer systems and associated components, such as telecommunications and storage systems.

Decentralized IT - information technology service and support organizations reporting to the heads of business units, departments, or programs that manage or support their own information systems.

Digital Data - the subset of Data (as defined above) that is transmitted by, maintained, or made available in electronic media.

Emergency Change - a change to an Information Resource made in response to unexpected events or circumstances that pose a threat to the environment or institution and thereby justify use of expedited change procedures.

Electronic Communication - method used to convey a message or exchange information via Electronic Media instead of paper media. It includes the use of Electronic Mail, instant messaging, Short Message Service (SMS), facsimile transmission, Social Media, and other paperless means of communication.

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

Electronic Media - any of the following:

- electronic storage media including storage devices in computers (hard drives, memory) and any removable/transportable digital storage medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, intranet, and the physical movement of removable/transportable electronic storage media.

Guideline - recommended, non-mandatory controls that help support Standards or serve as a reference when no applicable Standard is in place.

High Impact Information Resources - Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- result in major damage to organizational assets;
- result in major financial loss; or
- result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

High Risk Computing Device - a computing device meeting any of the following criteria:

- is located in a public or high-traffic area and is used by a person who has access to Confidential Data;
- is used to create, store, or process Confidential Data or is used within a functional area that handles such data;
- is used by any executive officers or their support staff; or
- contains data that if accessed, changed, or deleted by an unauthorized party could have highly adverse impact on the University or U. T. System.

  Based on these criteria, designation of a computing device as being “High Risk” is made by the Information Resource Owner in consultation with the Institution’s Information Security Officer. In event of disagreement regarding the designation of a computing device as being “High Risk,” the Information Resource Owner of the data placed at potential risk determines the classification of the device.

Information - Data organized, formatted and presented in a way that facilitates meaning and decision making. All information is comprised of data.

Information Resources - any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, Network Infrastructure, personal computers, notebook computers, hand-held computers, 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 Custodian (Custodian) - an individual, department, Institution, or third-party service provider responsible for supporting and implementing Information Resources Owner defined controls to Information Resources. Custodians include Information Security Administrators, institutional information technology/systems departments, vendors, and any third-party acting as an agent of or otherwise on behalf of an Institution.

Information Resources Manager (IRM) - the executive responsible for Information Resources across the whole of the institution as defined in Chapter 2054, Subchapter D, *Texas Government Code*.

Information Resources Owner (Owner) - the manager or agent responsible for the business function that is supported by the Information 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 and authorizing access to the Information Resource. 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. Note: In the context of this Information Security Policy and Standards, Owner is a role that has security responsibilities assigned to it by Texas Administrative Code (TAC) 202.72. It does not imply legal ownership of an Information Resource. All University Information Resources are legally owned by the University of Texas System or the member Institution.

Information Security Administrator - a departmental employee, designated by management, who assists with information security tasks as described in UTS165 Standard 1 - Information Resources Security Responsibilities and Accountability.

Information Security Program - the Policies, Standards, Procedures, Guidelines, elements, structure, strategies, objectives, plans, metrics, reports, resources, and services adopted for the purpose of securing University Information Resources.

Information System - an interconnected set of Information Resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, Network Infrastructure, information, data, applications, communications, and people.

Information Technology (IT) - the hardware, software, services, supplies, personnel, facilities, maintenance, and training used for the processing of Data and telecommunications.

Inherent Impact - the degree of Impact (High, Moderate, or Low) that could result if Information Resources were subjected to unauthorized access, use, disclosure, disruption, modification or destruction.

Institution - U. T. System Administration, UTIMCO, or any individual University that is part of the University of Texas System. Same as University.

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

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

Lead Researcher - the person engaged in the conduct of Research with primary responsibility for stewardship of Research Data on behalf of an Institution. For the purpose of this Policy and associated Standards, the term is synonymous with Principal Investigator.

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.

Low Impact Information Resources - Information resources whose loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to organizational assets;
- result in minor financial loss; or
- result in minor harm to individuals.

Malware - a computer program that is inserted into an Information System, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of data, applications, or operating system, or of otherwise annoying or disrupting the User or Information System. Malware (malicious software) may attach itself to a file or application; deliver a payload without the knowledge or permission of the User; insert itself as a service or process to intercept sensitive information and/or keystrokes and deliver it to a third-party; or compromise the User’s computer and use it to launch compromises against other computers, among other capabilities. Viruses, worms, Trojan horses, spyware, adware, ransomware, and any code-based entity that infects a host are examples of malicious software.

Mission Critical Information Resources - Information Resources defined by an Institution or State agency to be essential to U. T. System or the Institution’s ability to meet its instructional, research, patient care, or public service missions. The loss of these resources or inability to restore them in a timely fashion would result in the failure of U. T. System or Institution’s operations, inability to comply with regulations or legal obligations, negative legal or financial impact, or endanger the health and safety of faculty, students, staff, and patients. Mission Critical Information Resources include but are not limited to:

- Information Systems managing Confidential Data;
- Common Use Infrastructures;
- Institutional Network and Data Center Infrastructure;
- Identity and Access Management Systems, such as single-sign-on or other applications required to enable access to other critical system;
- Administrative systems (e.g., HR, Finance, Payroll, student/patient enrollment and billing, etc.);
- Student information systems;
- Patient care and life-support systems, etc.

Moderate Impact Information Resources - Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to organizational assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Network Infrastructure - the distributed hardware and software (i.e., cabling, routers, switches, wireless access points, access methods, and protocols), information, and integrating components that allow institutional network hosts to communicate with one another and enable the administrative, learning, research, and health care missions of the Institution.

Non-University Owned Computing Device - any device that is capable of receiving, transmitting, and/or storing electronic data, and that is not owned, leased, or under the management of an Institution including personally owned devices.

Owner – See Information Resources Owner.

Password - a string of characters used to verify or "authenticate" a person's identity. Passphrases and personal identification numbers (PIN) serve the same purpose as a Password.

Personally Identifiable Information (PII) - information that alone or in conjunction with other information identifies an individual. PII includes, but is not limited to: an individual’s name; a Social Security number; a date of birth; a government-issued identification number; a mother’s maiden name; unique biometric data (including an individual’s fingerprint, voice print, and retina or iris image); a unique electronic identification number, address, or routing code; or a telecommunication access device.

Policy - high level statements of intent relating to the protection of Information Resources across an organization (e.g., the U. T. System). Compliance with a Policy is mandatory.

Portable Computing Device - any easily movable device capable of receiving, transmitting, and/or storing data. These include, but are not limited to: notebook computers, handheld computers, tablets (e.g., iPads, etc.), PDAs (personal digital assistants), pagers, smartphones (e.g., iPhones, etc.), Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs, and similar storage devices.

Practice - customary actions, which may or may not be documented, taken to accomplish information security tasks.

Procedure - step by step instructions to assist information security and technology staff, Custodians, and Users in implementing various policies, standards, and guidelines.

Published Data - one of three data classifications within the U. T. System Data Classification Standard. This includes data and information made available to the public through posting to public websites or distribution through email, social media, print publications, or other media.

Remote Access - access to University Information Resources that originates from a Remote Location.

Remote Location - a location outside the physical boundary of the Institution (inclusive of University leased/rented properties and locations within the University's compliance environment).

Residual Risk - the risk (Low, Moderate, or High) that remains after security controls have been applied.

Research - systematic investigation designed to develop and contribute to knowledge and may include all stages of development, testing, and evaluation.

Researcher - Lead Researchers, faculty, staff, graduate students, postdoctoral fellows, residents, and visiting/affiliated scientists who are engaged in or responsible for Research activities.

Risk – a function of the likelihood that a threat will exploit a vulnerability and the resulting impact to University missions, functions, image, reputation, assets, or constituencies if such an exploit were to occur.

Scheduled Change - a change to an Information Resource made under normal working conditions following formally defined change control processes as defined in UTS165 Standard 7 - Change Management.

Security Incident - an event that results in unauthorized access, loss, disclosure, modification, disruption, or destruction of Information Resources whether accidental or deliberate.

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.

Social Media - a forum or media for social interaction, using highly accessible and scalable communication techniques. Examples include but are not limited to wikis (e.g., Wikia, Wikimedia); blogs and microblogs (e.g., Blogger, Twitter); content communities (e.g. Flickr, YouTube); social networking sites (e.g., Facebook, MySpace, LinkedIn); virtual game worlds; and virtual communities (e.g., SecondLife)

Standards - specific mandatory controls that are components of the Information Security Policy.

State Record – a document, book, paper, photograph, sound recording, or other material, regardless of physical form or characteristic, made or received by a state department or institution according to law or in connection with the transaction of official state business.

Strong Password - a Password constructed so that another User cannot easily guess it and so that a “hacker” program cannot break it within a reasonable amount of time. It typically consists of a minimum number of positions in length and contains a combination of alphabetic, numeric, or special characters.

Two-factor Authentication - a process for verifying a person’s identity that requires use of two of the following three elements:

(a) something the person knows, such as a password;

(b) something the person has, such as a token or smart card; or

(c) a unique characteristic of the person, such as a fingerprint.

University - U. T. System Administration, UTIMCO, or any of the academic Institutions, or health science centers, or other entities as from time to time may be assigned by specific legislative act to the governance, control, jurisdiction, or management of U. T. System that comprise The University of Texas System. Same as Institution.

University of Texas System (U. T. System) - the academic institutions and health science centers in The University of Texas System, plus U. T. System Administration and UTIMCO.

University of Texas System Administration (U. T. System Administration) - the central administrative offices that provide oversight and coordination of the activities of U. T. System and its Institutions.

University of Texas System Data (University Data) - All Data or Information held on behalf of U. T. System and its Institutions created as a result of and/or in support of U. T. System business, or residing on U. T. System Information Resources, including paper records.

U. T. System Shared Data Center - any data center governed by the U. T. Shared Data Center (SDC) group on behalf of the U. T. System including the

Arlington Data Center (ARDC) and the **Houston Data Center (HDC)**.

U. T. Systemwide Information Security Program – the U. T. System policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, resources, and services that establish requirements and provide for oversight and supplemental support for Institutional Information Security Programs.

User - an individual, automated application, or process that is authorized by the Owner to access the resource, in accordance with Federal and State law, university policy, and the Owner's procedures and rules. 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 the unauthorized disclosure of Confidential Data. 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.

UTIMCO - The University of Texas Investment Management Company that manages U. T. System's investment assets.

Vendor - any third-party that contracts with U. T. System or an Institution to provide goods and/or services to U. T. System or the Institution.

4. Relevant Federal and State Statutes and Regulations

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, and all regulations adopted to implement FERPA.

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, and all regulations adopted to implement HIPAA.

Health Information Technology for Economic and Clinical Health Act, (HITECH) Act of 2009, and all regulations adopted to implement HITECH.

Federal Privacy Act of 1974 (Section 7 of Pub. L. 93-579 in Historical Note), 5th U.S.C. § 552a

Social Security Act, 42 U.S.C. §§ 408(a)(8) and 405(c)(2)(C)(viii)(I)

Gramm-Leach-Bliley Act (GLBA Gramm-Leach-Bliley Act (GLBA)

Texas Government Code Section 2054.121

Texas Education Code Section 65.31

Texas Business and Commerce Code Chapter 521

Texas Government Code Section 559.003

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C.§§202.1-202.4, 202.70-202.76

5. Relevant System Policies, Procedures, and Forms

U. T. System Information Security Integrated Controls Framework

U. T. System Identity Management Federation Member Operating Practices (MOP)

6. System Administration Office(s) Responsible for Policy

The University of Texas Systemwide Office of Information Security
Telephone Number: 512-499-4389
Email: ciso@utsystem.edu

7. Dates Approved or Amended

April 12, 2007
Amended June 15, 2010
Amended June x, 2011
Amended March 16, 2015

8. Contact Information

Questions or comments about this policy should be directed to:
bor@utsystem.edu