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
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. Who Should Know

All individuals accessing, managing, or possessing U. T. System Information Resources including U. T. System staff, faculty, and students, as well as Vendors and contractors providing services on behalf of U. T. System and other third-party contractors.

7. 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

8. Dates Approved or Amended

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

9. Contact Information

Questions or comments about this policy should be directed to:
bor@utsystem.edu
UTS165 Standard 1: Information Resources Security Responsibilities and Accountability.

1.1 Designation of Responsibility. All Institutions and any U. T. System governing body having oversight of Information Resources must have designated and documented roles and responsibilities for the information security function.

1.2 Chancellor. The Chancellor shall:

(a) designate an individual to serve as U. T. System Chief Information Security Officer (CISO);

(b) budget sufficient resources to fund ongoing information security remediation, implementation, and compliance activities that reduce compliance Risk to an acceptable level; and

(c) ensure that appropriate corrective and disciplinary action is taken in the event of noncompliance.

1.3 Chief Administrative Officers. The Chief Administrative Officer at each Institution shall:

(a) ensure the Institution’s compliance with this Policy and associated Standards;

(b) designate an individual to serve as the Institutional Information Security Officer (ISO) who shall:

1. serve in the capacity as required by 1 Texas Administrative Code 202.71 (b) with authority for that entire Institution;

2. report to the President or to a senior executive, other than the Chief Information Officer or Information Resources Manager, who reports to the President; and

3. have a dotted line reporting relationship to the Institution’s Compliance Officer and the U. T. System Chief Information Security Officer;

(c) budget sufficient resources to fund ongoing information security remediation, implementation, and compliance activities (e.g., staffing, training, tools, and monitoring activities) that reduce compliance Risk to documented acceptable levels;

(d) approve the Institution’s Information Security Program; and
(e) ensure appropriate corrective and disciplinary action is taken in the event of noncompliance.

1.4 Information Resources Manager. The IRM shall:

(a) implement security controls in accordance with the Institutional Information Security Program; and

(b) review and approve or disallow the purchase or deployment of new Decentralized IT Information Systems or services (e.g., electronic mail/web/file Servers, file/system Backup, storage, etc.) that duplicate services provided by Centralized IT.

1.5 U. T. System Chief Information Security Officer (U. T. System CISO). The U. T. System Chief Information Security Officer shall:

(a) provide leadership, strategic direction, and coordination for the U. T. Systemwide Information Security Program including issuing of Policies, Standards, Procedures, and Guidelines;

(b) chair and hold meetings of the U. T. System CISO Council at least quarterly;

(c) develop and oversee the U. T. Systemwide Information Security Compliance Program;

(d) provide guidance relating to Institutional and Common Use Infrastructures Information Security Programs regarding organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum Standards;

(e) define the Risk management process to be used for U. T. System information security Risk management activities, and ensure performance of Risk assessment for systemwide systems that will process or store Confidential Data;

(f) explore and recommend the acquisition of cybersecurity tools, resources, and services that can be utilized by multiple U. T. Institutions and for ways to share expertise among Institutions;

(g) establish reporting requirements, metrics, and timelines and monitor effectiveness of security strategies at each Institution;

(h) apprise the Chancellor, the U. T. System Executive Compliance Committee, and the Board of Regents on the status and effectiveness of the Information Security Compliance Programs;
(i) oversee and/or monitor deployment of information security initiatives funded or sponsored through the U. T. System, and manage contracts with service providers;

(j) establish processes for assessing information security proposals for U. T. System sponsorship, and oversee procurements; and

(k) appoint an Information Security Officer for Common Use Infrastructures.

1.6 Information Security Officer for Common Use Infrastructures. The Information Security Officer for Common Use Infrastructures is responsible for defining, implementing, and managing an Information Security Program encompassing the U. T. System Common Use Infrastructures in accordance with requirements of the U. T. Systemwide Information Security Program and shall:

(a) develop and maintain a current and comprehensive Information Security Program, that includes Risk assessment, metrics, action plans, training plans, monitoring plans, and adoption of Policies, Standards, Procedures, and/or Guidelines as needed;

(b) coordinate with Institutional Information Security Officers, Information Resource Managers, facilities management, and governance groups to ensure appropriate Policies, Standards, Procedures, and/or Guidelines are established, and responsible parties are assigned;

(c) monitor the effectiveness of security controls and submit required reports to the U. T. System Chief Information Security Officer; and

(d) serve as a member of the U. T. System Chief Information Security Officer Council, and perform other tasks similar in nature to an Institutional Information Security Officer.

1.7 Institutional Information Security Officer (Institutional ISO). The Institutional Information Security Officer is the individual responsible for an Institution's Information Security Program and shall:

(a) work in partnership with the University community, constituency groups, and leadership to establish effective and secure processes and information systems and to promote information security as a core institutional value;

(b) provide information security oversight for all Centralized and Decentralized IT Information Resources;
(c) develop and maintain a current and comprehensive Information Security Program, that includes Risk assessment, action plans, training plans, monitoring plans, and specific Risk mitigation strategies to be used by Owners and Custodians of Mission Critical Information Resources to manage identified Risks;

(d) develop Institutional Policies, Standards, Procedures, and/or Guidelines to ensure that the protection of Information Resources is considered during the development or purchase of new computer applications or services;

(e) develop or adopt a Data Classification Standard that conforms or maps to UTS165 Standard 9 – Data Classification;

(f) coordinate Risk assessments required by U. T. System to be reported to the U. T. System Executive Compliance Committee or Board of Regents, and ensure that annual information security Risk assessments are performed and documented by Owners of Mission Critical Information Resources and Information Resources containing Confidential Data in accordance with UTS165 Standard 10 – Risk Management;

(g) ensure that each Owner of Mission Critical Information Resources has designated an Information Security Administrator (ISA);

(h) establish an Institutional Information Security Working Group composed of ISAs (ISA Working Group) and convene meetings at least quarterly;

(i) approve and document any exceptions to information security Policies or Standards, other than UTS165 Standard 2 – Acceptable Use of Information Resources, within the Institution in accordance with UTS165 Standard 23 – Security Control Exceptions;

(j) document and justify, in collaboration with the Owners, exceptions to specific elements of the program required due to circumstances within a specific organizational unit(s) within an Institution, and include such exceptions in the annual report to the Chief Administrative Officer;

(k) establish reporting requirements, metrics, and timelines, and monitor effectiveness of security strategies implemented in both Centralized and Decentralized IT;

(l) perform, at a minimum, an annual vulnerability assessment of Information Resources maintained in both Centralized and
Decentralized IT and track implementation of any remediation required as a result of the assessment;

(m) ensure that an annual external network penetration test is performed and track implementation of needed Risk remediation;

(n) specify and require use of appropriate security software such as anti-Malware, firewall, configuration management, and other security related software on Computing Devices owned, leased, or under the custody of any department, operating unit, employee, or other individual providing services to the Institution;

(o) establish and communicate security configuration requirements and Guidelines;

(p) ensure Computing Devices are administered by appropriately trained staff and in accordance with Policies, Standards, and Procedures;

(q) review the security requirements, specifications, and third-party Risk assessments of any new computer applications or services that receive, maintain, and/or share Confidential Data;

(r) approve security requirements for the purchase of Information Technology hardware, software, and systems development services;

(s) ensure all employees receive periodic information security training appropriate to the security role (such as Owner or ISA) of the employee, including high-level information security awareness training as part of each employee’s first-time compliance training;

(t) communicate instances of noncompliance to appropriate administrative officers for corrective, restorative, and/or disciplinary action;

(u) investigate Security Incidents and inform the Chief Administrative Officer of incidents posing significant Risk to individuals, the Institution, or other organizations;

(v) report Significant Information Security Incidents, as defined by the U. T. System Security Incident Reporting Requirements, to the U. T. System CISO;

(w) participate in the U. T. System CISO Council meetings, workgroups, and related activities;
(x) report to the U. T. System CISO in accordance with Program reporting guidance and metrics;  
(y) provide updates to the Institutional Compliance Committee regarding information security Risks and issues; and  
(z) provide a report, at least annually, to the Chief Administrative Officer with copies to the Institution’s Chief Information Officer and Compliance Officer and the U.T. System CISO on the status and effectiveness of Information Resources security controls for the whole Institution in accordance with reporting instructions provided by the U. T. System Chief Information Security Officer.

1.8 Department Heads and Lead Researchers. Department Heads and Lead Researchers at each Institution shall classify and appropriately secure Data under their control including Data held in relation to subcontracts for projects in which the prime award is at another Institution or agency.

1.9 Information Resources Owners. For Information Resources and Data under their authority, Owners shall:

(a) grant access to Information Systems and Data;  
(b) control and monitor access to Data based on Data sensitivity and Risk;  
(c) classify Data based on the Institution’s Data Classification Standard;  
(d) conduct Risk assessments that identify the Information Resources under their authority and the level of Risk associated with the Information Resources and the vulnerabilities, if any, to the Institution’s information security environment;  
(e) define, recommend, and document acceptable Risk levels for Information Resources and Risk mitigation strategies;  
(f) document and justify, in collaboration with the ISO, any exceptions to specific program requirements due to extenuating circumstances within the Owner's area of responsibility;  
(g) ensure that Data is securely backed up in accordance with Risk management decisions;  
(h) ensure that Data is maintained in accordance with the applicable University records retention schedule and Procedures;
(i) provide documented permission and justification for any User who is to store Confidential University Data on a Portable Computing Device or a Non-University Owned Computing Device;

(j) ensure that High Risk Computing Devices and Confidential Data are encrypted in accordance with requirements specified in UTS165 Standard 11 - Safeguarding Data;

(k) ensure that Information Resources under their authority are administered by qualified Information Resources Custodians;

(l) ensure that a Risk assessment is performed prior to purchase of any software that has not been previously assessed by the Institution for use under similar circumstances;

(m) ensure that a third-party Risk assessment is performed prior to purchase of Vendor services that involve hosting or accessing University Data; and

(n) ensure that contracts involving products or services that impact Information Resources contain information security language appropriate to the Risk.

1.10 Owner of Mission Critical Information Resources. For Information Resources under the Owner's authority, the Owner shall:

(a) designate an individual to serve as an Information Security Administrator (ISA) to implement information security Policies and Procedures and to report incidents to the ISO;

(b) provide for appropriate training for ISAs to ensure effective security Practices;

(c) perform an annual information security Risk assessment that identifies Information Resources, levels of associated Risk, and any vulnerabilities to those Information Resources;

(d) define, recommend, and document acceptable Risk levels for Information Resources and Risk mitigation strategies as needed; and

(e) adopt a disaster recovery plan for Information Resources and ensure testing is performed in accordance with the requirements of UTS165 Standard 6 - Backup and Disaster Recovery.

1.11 Information Resources Custodians. Information Resources Custodians shall:
(a) implement approved Risk mitigation strategies and adhere to information security Policies and Procedures to manage Risk levels for Information Resources under their care;

(b) implement monitoring controls for detecting and reporting incidents;

(c) control and monitor access to Information Resources under the Custodian’s care based on sensitivity and Risk;

(d) implement and adhere to approved Institutional Change Management processes to ensure secure, reliable, and stable operations;

(e) encrypt High Risk Computing Devices and Confidential Data in accordance with requirements specified in UTS165 Standard 11 - Safeguarding Data;

(f) provide appropriate technical training to employees providing Information Technology, security, help-desk, or technical support for Information Resources under their responsibility; and

(g) ensure that technical staff under their authority are qualified to perform their assigned duties.

1.12 Information Security Administrator. Information Security Administrators shall:

(a) implement and comply with all IT Policies and Procedures relating to assigned Information Systems;

(b) assist Owners in performing annual information security Risk assessments;

(c) report general computing and Security Incidents to the Institutional ISO;

(d) as a member of the ISA Work Group, assist the Institutional ISO in developing, implementing, and monitoring the Information Security Program, and in establishing reporting guidance, metrics, and timelines for the ISO to monitor effectiveness of security strategies; and

(e) report at least annually to the Institutional ISO about the status and effectiveness of Information Resources security controls.

1.13 Institutional Offices with Designated Responsibility for Account Management. Each office within the Institution responsible for account management shall manage accounts in accordance with this UTS 165 and
all other applicable U. T. System and Institutional information security Policies, Standards, and Procedures.

1.14 Institutional Office Designated with Responsibility for Network Infrastructure. Each office so designated shall be responsible for:

(a) configuring and managing network resources in accordance with this UTS 165 and all other applicable U. T. System and Institutional information security Policies, Standards, and Procedures;

(b) segmenting the Institutional network physically or logically to reduce the scope of potential exposure of Information Resources in the event of a Security Incident;

(c) separating Internet facing applications from internal applications;

(d) maintaining appropriate access to the Network Infrastructure in accordance with this UTS 165 and all other applicable U. T. System and Institutional information security Policies, Standards, and Procedures;

(e) managing, testing, and updating operating systems and applications for network equipment for which it is responsible; and

(f) approving all access methods, installation of all network hardware connected to the local-area network and methods and requirements for attachment of any Non-U. T. System Owned Computer Systems or Devices to the U. T. System network.

1.15 Institutional Office Charged with Supporting Information Resources. The offices so designated shall be responsible for:

(a) formalizing best Practice Change Management processes into Practice Standards;

(b) requiring compliance from all individuals who manage Information Systems or applications; and

(c) providing support, guidance, and problem resolution to Owners, including Department Heads and Lead Researchers, and Users with respect to this Policy and applicable Standards, Policies, and Procedures.

1.16 Users.

(a) All Users must comply with this U. T. System Policy for Use and Security of Information Resources (UTS165). Users who fail to
comply are subject to disciplinary action in accordance with UTS165 Standard 24 – Disciplinary Actions.

(b) All Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University, must formally acknowledge and comply with the Institution’s Acceptable Use Policy as directed in UTS165 Standard 2 – Acceptable Use of Information Resources.
UTS165 Standard 2: Acceptable Use of Information Resources.

2.1 Acceptable Use Policy Requirement. All Institutions must adopt and incorporate for all purposes the U. T. System model Acceptable Use Policy that follows.

The University of Texas

INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY AGREEMENT

All individuals granted access to or use of System Information Resources must be aware of and agree to abide by the following acceptable use requirements:

**Definitions**
- **University**: The University of Texas
- **System**: The University of Texas System.
- **University Information Resources**: All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf.
- **University Data**: All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paper records.
- **Confidential Data or Confidential Information**: All University Data that is required to be maintained as private or confidential by applicable law.
- **User**: Any individual granted access to University Information Resources.

**General**
- University Information Resources are provided for the purpose of conducting the business of University and/or System. However, Users are permitted to use University Information Resources for use that is incidental to the User’s official duties to University or System (Incidental Use) as permitted by this policy.
- Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University have no expectation of privacy regarding any University Data they create, send, receive, or store on University owned computers, servers, or other information resources owned by, or held on behalf of, University. University may access and monitor its Information Resources for any purpose consistent with University’s duties and/or mission without notice.
- Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device.
- All Users must comply with applicable University and System Information Resources Use and Security policies at all times.
- Users shall never use University Information Resources to deprive access to individuals otherwise entitled to access University Information, to circumvent University computer security measures; or, in any way that is contrary to the University’s mission(s) or applicable law.
- Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User’s official duties as an employee of University and is approved in writing by the President or a specific designee. Viewing, access to, or storage or transmission of sexually explicit materials as Incidental Use is prohibited.
- Users must clearly convey that the contents of any email messages or social media posts that are the result of Incidental Use are not provided on behalf of the University and do not express the opinion or position of University. An example of an adequate disclaimer is: “The opinions expressed are my own, and not necessarily those of my employer, The University of Texas.”
- Users should report misuse of University Information Resources or violations of this policy to their supervisors.

**Confidentiality & Security of Data**
- Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with University’s Records Retention Policy and Records Management Guidelines.
- Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official University duties.
- Whenever feasible, Users shall store Confidential Information or other information essential to
the mission of University on a centrally managed server, rather than a local hard drive or portable device.

- In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, the User must ensure the data is encrypted in accordance with University, System's and any other applicable requirements.

- The following University Data must be encrypted during transmission over an unsecured network: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver's License Numbers and other government issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other University Data about an individual likely to expose the individual to identity theft. Email sent to and received from System and U.T. System institutions using University and/or System provided email accounts is automatically encrypted. The Office of Information Technology [or other applicable office] will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations.

- Users who store University Data using commercial cloud services must use services provided or sanctioned by University, rather than personally obtained cloud services.

- Users must not use security programs or utilities except as such programs are required to perform their official duties on behalf of University.

- All computers connecting to a University's network must run security software prescribed by the Information Security Officer as necessary to properly secure University Resources.

- Devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the University from a University network without notice.

### Email

- Emails sent or received by Users in the course of conducting University business are University Data that are subject to state records retention and security requirements.

- Users are to use University provided email accounts, rather than personal email accounts, for conducting University business.

- The following email activities are prohibited when using a University provided email account:
  - Sending an email under another individual’s name or email address, except when authorized to do so by the owner of the email account for a work related purpose.
  - Accessing the content of another User’s email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User’s official duties on behalf of University.
  - Sending or forwarding any email that is suspected by the User to contain computer viruses.
  - Any Incidental Use prohibited by this policy.
  - Any use prohibited by applicable University or System policy.

### Incidental Use of Information Resources

- Incidental Use of University Information Resources must not interfere with User’s performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or System policy.

- Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including University email accounts.

- A User’s incidental personal use of Information Resources does not extend to the User’s family members or others regardless of where the Information Resource is physically located.

- Incidental Use to conduct or promote the User’s outside employment, including self-employment, is prohibited.

- Incidental Use for purposes of political lobbying or campaigning is prohibited.

- Storage of any email messages, voice messages, files, or documents created as Incidental Use by a User must be nominal (less than 5% of a User’s allocated mailbox space).

- Files not related to System business may not be stored on network file servers.

### Additional Requirements for Portable and Remote Computing

- All electronic devices including personal computers, smart phones or other devices used to access or store University Information Resources, including email, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.

- University Data created or stored on a User’s personal computers, smart phones or other devices, or in databases that are not part of University’s Information Resources are subject to
Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources

• University issued mobile computing devices must be encrypted.
• Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted.
• University Data created and/or stored on personal computers, other devices and/or non-University data bases should be transferred to University Information Resources as soon as feasible.
• Unattended portable computers, smart phones and other computing devices must be physically secured.
• All remote access to networks owned or managed by University or System must be accomplished using a remote access method approved by the University or System, as applicable.

Password Management

• University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.
• Each User is responsible for all activities conducted using the User’s password or other credentials.

User Acknowledgment

I acknowledge that I have received and read the Information Resources Acceptable Use Policy. I understand and agree that my use of University Information Resources is conditioned upon my agreement to comply with the Policy and that my failure to comply with this Policy may result in disciplinary action up to and including termination of my employment.

Signature: ________________________________________________     Date__________________________
Print Name:_______________________________________________

2.2 Any deviations in an Institution’s Acceptable Use Policy from the U. T. System model Acceptable Use Policy must be reviewed and approved by the U. T. System Office of General Counsel.

2.3 The Acceptable Use Policy must address the following User responsibilities and behaviors:

(a) Ownership of U. T. System and the Institution’s Information Resources and Data, including Data maintained or created on a User’s personal devices;

(b) Incidental use of Information Resources, including impact of placement of personal Data on the Institution’s Information Resources;

(c) User’s expectations with regard to the privacy of information stored or created on U. T. System’s and the Institution’s Information Resources; and
(d) User’s responsibilities with respect to maintaining the security, integrity, and, as applicable, confidentiality of U. T. System’s and the Institution’s Information Resources.

2.4 Each Institution is responsible for ensuring that each User who is employed by the University or who provides services to or on behalf of the University acknowledges awareness of the existence of and the User’s responsibility for complying with the Institution’s Acceptable Use Policy.
UTS165 Standard 3: Information Security Programs.

3.1 Information Security Program Requirement. Each Institution and any governing body with oversight for Common Use Infrastructures must establish and maintain a Security Program that includes appropriate protections, based on risk, for all Information Resources including outsourced resources, owned, leased, or under the custodianship of any governing body or department, operating unit, or employee of the Institution.

3.2 Information Security Program. Each Security Program must include and document the following:

(a) annual risk assessment;

(b) current inventory of
   i. institution-owned or managed computing devices deployed throughout the institution, and
   ii. Mission-Critical applications and applications containing Confidential Data;

(c) strategies to address identified risks to Mission Critical Information Resources and Confidential Data;

(d) annual action plan, training plan, and monitoring plan; and

(e) metrics, reports, and timelines established by the U. T. System Office of Information Security.

3.3 Collection of Information Security Metrics. Each Institution must collect required metrics data in ways that are documented and verifiable.


4.1 Access Management Requirement.

(a) All Institutions must adopt Access Management processes to ensure that access to Information Resources is restricted to authorized Users.

(b) All Institutional offices or departments that create access accounts for networks or applications must manage the accounts in accordance with defined processes and the requirements of the U. T. System Identity Management Federation Member Operating Practices (MOP).


(a) assigning a unique identifier for each applicant, student, employee, insured dependent, research subject, patient, alumnus, donor, contractor, and other individuals, as applicable, at the earliest possible point of contact between the individual and the Institution;

(b) creating uniquely identifiable accounts for all Users. This includes accounts created for use by Vendors (see Standard 22);

(c) disabling all generic and default accounts;

(d) reviewing, removing and/or disabling accounts at least quarterly, or more often if warranted by Risk, to reflect current User needs or changes of User role or employment status;

(e) expiring Passwords or disabling accounts based on Risk; and

(f) managing access from wired and wireless devices, and from Remote Locations.


(a) establish and communicate to Users the roles and conditions under which Remote or wireless Access to Information Resources containing Confidential Data is permitted;

(b) require the use of secure and encrypted connections when accessing Information Resources containing Confidential Data across the Internet, or across open segments of the Institution.
network or wireless network (e.g., use of VPN for access, SFTP for transfers, encrypted wireless); and

(c) require monitoring for, identifying, and disabling of unauthorized (i.e., rogue) wireless access points.

4.4 Access to Institutional Networks. Through appropriate use of administrative, physical, and technical controls, the Institutional office or offices charged with maintaining the Network Infrastructure at each Institution are required to establish processes for approval of all network hardware connected to the Institutional or the U. T. System network and the methods and requirements for attachment, including any Non-U. T. System Owned Computer Systems or Devices, to ensure that such access does not compromise the operations and reliability of the network, or compromise the Integrity or use of Information contained within the network.

4.5 Data Access Control Requirement. All Owners and Custodians must control and monitor access to Data within their scope of responsibility based on Data sensitivity and Risk, and through use of appropriate administrative, physical, and technical safeguards including the following:

(a) Owners must limit access to records containing Confidential Data to those employees who need access for the performance of the employees’ job responsibilities. An employee may not access Confidential Data if it is not necessary and relevant to the employee’s job function.

(b) Owners and Custodians must monitor access to records containing Confidential Data by the use of appropriate measures as determined by applicable Policies, Standards, Procedures, and regulatory requirements.

(c) Owners and Custodians must establish log capture and review processes based on Risk and applicable Policies, Standards, Procedures, and regulatory requirements. Such processes must define:

i. the Data elements to be captured in logs;

ii. the time interval for custodial review of the logs; and

iii. the appropriate retention period for logs.

(d) Employees may not disclose Confidential Data to unauthorized persons or Institutions except:
i. as required or permitted by law, and, if required, with the consent of the Data Owner;

ii. where the third-party is the agent or contractor for the Institution and the safeguards described in Standard 4.6 are in place to prevent unauthorized distribution; or

iii. as approved by the Institution’s legal office or the Office of General Counsel.

4.6 Access for Third-Parties. If an Institution intends to provide University Data to a third-party acting as an agent of or otherwise on behalf of that Institution (example: an application service provider) a written agreement with the third-party is required.

(a) Such third-party agreements must specify:

i. the Data authorized to be accessed;

ii. the circumstances under and purposes for which the Data may be used; and

iii. that all Data must be returned to the Institution, or destroyed, in a manner specified by the Institution upon end of the third-party engagement.

(b) If the Institution determines that its provision of Data to a third-party will result in significant Risk to the confidentiality, Integrity, or availability of such Data, the agreement must specify terms and conditions, including appropriate administrative, physical, and technical safeguards for protecting the Data.

4.7 Two-factor Authentication Requirements. Effective August 31, 2015, Two-factor Authentication is required in the following situations:

(a) when an employee or other individual providing services on behalf of the University (such as a student employee, contractor, or volunteer) logs on to a University network using an enterprise Remote Access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;

(b) when an individual described in (a) who is working from a Remote Location uses an online function such as a web page to modify employee banking, tax, or financial Information; or

(c) when a Server administrator or other individual working from a Remote Location uses administrator credentials to access a Server that contains or has access to Confidential University Data.
UTS165 Standard 5: Administrative/Special Access Accounts.

Each Institution must adopt Institutional Standards and/or Procedures to ensure that all administrative/special access accounts with elevated access privileges on computers, network devices, or other critical equipment (example: accounts used by system administrators and network managers) are used only for their intended administrative purpose and to ensure that all authorized Users are made aware of the responsibilities associated with use of privileged special access accounts. These Procedures must address:

(a) acceptable use of administrative/special access accounts and intended administrative purposes;

(b) authorization required for use of administrative/special access accounts;

(c) the need to review, remove, and/or disable administrative/special access accounts at least annually, or more often if warranted by Risk, to reflect current authorized User needs or Changes of User role or employment, or other status conferring access; and

(d) the need to escrow login Passwords for each secured system for access during emergencies. Individual User login Passwords shall not be escrowed.
UTS165 Standard 6: Backup and Disaster Recovery.

6.1 Backup Plan Requirement. All U. T. System Data, including Data associated with research, must be backed up in accordance with Risk management decisions implemented by the Data Owner. Each Institution’s Backup plan must incorporate Procedures for:

(a) recovering Data and applications in case of events such as natural disasters, system disk drive failures, espionage, Data entry errors, human error, or system operations errors;

(b) assigning operational responsibility for backing up of all Servers;

(c) scheduling Data Backups and establishing requirements for off-site storage;

(d) securing on-site/off-site storage and Media in transit; and

(e) testing Backup and recovery Procedures.

6.2 Disaster Recovery Plan. Owners of Mission Critical Information Resources and of Information Resources containing Confidential Data must adopt a disaster recovery plan commensurate with the Risk and value of the Information Resource and Data. The disaster recovery plan must incorporate Procedures for:

(a) recovering Data and applications in the case of events that deny access to Information Resources for an extended period (e.g., natural disasters, terrorism);

(b) assigning operational responsibility for recovery tasks and communicating step-by-step implementation instructions;

(c) testing the disaster recovery plan and Procedures every two years at minimum; and

(d) making the disaster recovery plan available to the Institutional ISO and other stakeholders.
7.1 Change Management Requirement. All Institutions must adopt Change Management processes to ensure secure, reliable, and stable operations to which all offices that support Mission Critical Information Resources or Network Infrastructures are required to adhere. The Change Management process must incorporate Procedures for:

(a) formal identification, classification, prioritization, and request of Scheduled Changes;

(b) identification and deployment of Emergency Changes;

(c) assessment of potential impacts of changes, including the impact on Data classification, Risk assessment, and other security requirements;

(d) authorization of changes and exceptions;

(e) testing changes;

(f) change implementation and back-out planning; and

(g) documentation and tracking of changes.

7.2 Information Resources Custodians. All Custodians must implement and adhere to approved institutional Change Management processes to ensure secure, reliable, and stable operations.
UTS165 Standard 8: Malware Prevention.


8.2 All computing devices owned, leased, or under the control of U. T. System Institutions must, to the extent technology permits, execute and keep up to date all required protection software and adhere to any other protective measures as required by applicable Policies and Procedures.

8.3 Any personally owned Computing Device that contains Confidential University Data must be configured to comply with required University security controls while holding such Data.

8.4 Any personally owned Computing Device that connects to a University network must be configured to comply with required University security controls while connected to such network.
UTS165 Standard 9: Data Classification.

9.1 Data Classification Standard. Each Institution within the U. T. System shall establish an Institutional Data Classification Standard that conforms to or maps to the U. T. System Data Classification Standard defined in 9.5 of this Standard.

9.2 Data Discovery. Institutional ISOs must develop a plan for identifying Digital Data maintained in both Centralized and Decentralized IT.

9.3 Classification Responsibility. Owners of Information Resources within the Institution must classify Data based on the Institutional Data Classification Standard.

9.4 The U. T. System Data Classification Standard is to be used to assess Data confidentiality, Integrity, and availability requirements for Data to be stored or processed within U. T. System Common Use Infrastructures.

9.5 The University of Texas System Data Classification Standard consists of three mutually exclusive Data classifications based on fit within a spectrum indicating the degree to which access to the Data must be restricted and Data Integrity and availability must be preserved. The three classifications are as follows:

<table>
<thead>
<tr>
<th>Data Classification and Description</th>
<th>Examples</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidential</strong> Information / Data</td>
<td>Patient billing Information and Protected Health Information subject to HIPAA or applicable state law.</td>
<td>Information (Data) cannot simply be declared to be “Confidential.” This classification is reserved for Information that is protected from public release based on State or Federal law, or a legally binding order or agreement. Likewise, Data cannot be declared to be “Confidential” under all circumstances. Context is an essential element.</td>
</tr>
<tr>
<td></td>
<td>Student education records subject to FERPA.</td>
<td>(In relation to the Federal Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, this category equates to HIGH IMPACT for a Confidentiality, Integrity, and Availability breach)</td>
</tr>
<tr>
<td></td>
<td>A credit card number associated with an individual’s name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A social security number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medical Research Data that contains protected health information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Certain student loan Information subject to the Gramm Leach Billey Act.</td>
<td></td>
</tr>
<tr>
<td><strong>Controlled</strong> Information / Data</td>
<td>Operational records, operational statistics, employee salaries, budgets, expenditures.</td>
<td>This classification likely encompasses the greatest volume of Data within the University.</td>
</tr>
<tr>
<td>The Controlled classification</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The University of Texas System Information Resources Use and Security Policy

Policy: UTS165

Page 36 of 65
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>FIPS 199 Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Communications</td>
<td>Internal communications that do not contain Confidential Information. Research Data that has not yet been published, but which does not contain Confidential Information protected by law.</td>
<td>(In terms of FIPS 199, this category equates to MODERATE IMPACT for a Confidentiality, Integrity, and Availability breach)</td>
</tr>
<tr>
<td>Published Information/Data</td>
<td>Published Information/Data includes all Data made available to the public through posting to public websites, distribution through Email, Social Media, print publications, or other Media. Statistical reports, Fast Facts, Published Research, unrestricted directory Information, educational content available to the public at no cost.</td>
<td>Information can migrate from one classification to another based on Information life-cycle. Unpublished Research may fit the criteria of “Controlled Information” until published upon which it would become Published Information. (In terms of FIPS 199, this category equates to LOW IMPACT for a Confidentiality, Integrity, and Availability breach.)</td>
</tr>
</tbody>
</table>
UTS165 Standard 10: Risk Management.

10.1 Each Institution must maintain an accurate inventory of Information Resources and identify Owners.

10.2 Information Resources Owners. For Information Resources under the Owners’ authority, Owners must:

(a) in consultation with the Institutional Information Security Officer, define, approve, and document acceptable Risk levels and Risk mitigation strategies; and

(b) conduct and document Risk assessments to determine Risk and the Inherent Impact that could result from their unauthorized access, use, disclosure, disruption, modification, or destruction. Timing of assessments shall be:

   i. annually for all Mission Critical Information Resources and Information Resources containing Confidential Data; and

   ii. at periodic time intervals to be defined by the Resource Owner in consultation with the Institutional Information Security Officer for non-Mission Critical Information Resources and Information Resources not containing Confidential Data.


10.4 Institutional Information Security Officer. Institutional ISOs must ensure that annual Information Security Risk assessments are performed and documented by each Owner of Mission Critical Information Resources or Information Resources containing Confidential Data.

10.5 Sponsored Projects. Principal Investigators must perform reviews, in collaboration with the Institutional ISO, of the implementation of required security controls (i.e. control objectives, controls, Policies, processes, and Procedures for Information security) for sponsored projects under their authority. Assessments for sponsored projects must be performed annually based on Risk.

10.6 Risk Assessment of Third-party Service Providers. A third-party Risk assessment is required in the following situations:

(a) when purchasing services that result in exchange of University Data or hosting of University Information Systems with a Vendor or other organization; or
(b) when purchasing systems or software, whether it is to be hosted on premises or at a Vendor facility, if Confidential University Data will be stored within or processed by the system or software.

10.7 U. T. System Information Security Risk Assessment Framework and Assessments. Information Security Risk Assessments that are to be aggregated for systemwide reporting to the U. T. System Executive Compliance Committee and/or the U. T. System Board of Regents shall be conducted using a risk management framework and process defined by U. T. System Office of Information Security and shall be coordinated at the Institutional level by the Institutional ISO.

10.8 Risk Acceptance. Decisions relating to acceptance of Risk must be documented and are to be made by:

(a) the Information Resource Owner, in consultation with the Institutional Information Security Officer or designee, for resources having a residual Risk of Low or Moderate.

(b) the Chief Administrative Officer, or designee, considering recommendations of the Owner and Institutional Information Security Officer, for resources having a residual Risk of High.
UTS165 Standard 11: Safeguarding Data.

11.1 Protection Requirement. Each Institution’s Policies, Standards, and/or Procedures must describe and require steps to protect University Data using appropriate administrative, physical, and technical controls in accordance with the Institutional Information Security Program and Data Classification Standard, and UTS165 and its associated Standards.

11.2 Non-University Third-Party Storage Services. University Data must not be stored on personally procured third-party (e.g. Cloud) storage services.

11.3 Password and Encryption Protection for Computing Devices and Data.

(a) Desktop Computers.

i. All High Risk Desktop Computers owned, leased, or controlled by the University must be Password protected and encrypted using methods approved by the Institution’s Information Security Officer.

ii. All desktop computers purchased after September 1, 2013 must be Password protected and encrypted using methods approved by the Institution’s Information Security Officer before their deployment.

(b) Laptop Computers and Other Mobile Devices.

i. All laptop computers and other mobile devices, including but not limited to mobile and smartphones, and tablet computers that are owned, leased, or controlled by the University, must be encrypted using methods approved by the Institution’s Information Security Officer.

ii. USB thumb drives and similar removable storage devices owned, leased, or controlled by the University must be encrypted before storage of any Confidential University Data on the device.

(c) Personally Owned Devices. All personally owned computers, mobile devices, USB thumb drives, or similar devices must be Password protected and encrypted using methods approved by the Institution’s Information Security Officer if they contain any of the following types of University Data:

i. Information made confidential by Federal or State law, regulation, or other legally binding order or agreement;
ii. Federal, State, University, or privately sponsored Research that requires confidentiality or is deemed sensitive by the funding entity; or

iii. any other Information that has been deemed by the U. T. System or a U. T. System Institution as essential to the mission or operations of System to the extent that its Integrity and security should be maintained at all times.

11.4 Assured Access to Encrypted Data.

(a) For University owned, leased, or controlled devices, the Institution must use processes to ensure an ability to access encrypted Data in the event that an encryption key becomes corrupted.

(b) For personally owned devices, the device owner is responsible for ensuring that encrypted Data is backed up to University owned or sanctioned storage using processes prescribed by the Institution.

11.5 Protecting Data in Transit. All Institutions shall adopt Policies, Standards, and/or Procedures and implement appropriate administrative, physical, and technical safeguards necessary to adequately protect the security of Data during transport and electronic transmissions. Each of the following shall be addressed:

(a) identification and transmission of the least amount of Confidential Data required to achieve the intended business objective;

(b) encryption of all Confidential Data transmitted over the Internet;

(c) encryption of all Confidential Data transmitted between Institutions and Shared Data Centers; and

(d) deletion of transmitted and received Confidential Data upon completion of the intended business objective.

11.6 Protecting Common Use Information Resources.

(a) The ISO for Common Use Infrastructures is responsible for implementation of an Information Security Program for Common Use Infrastructures, and for documenting associated roles and responsibilities.

(b) For services provided via Common Use Infrastructures, Memorandum of Understanding (MOU) documents between U. T. System and host Institutions, and between U. T. System and participant Institutions must identify roles and responsibilities for provision of Information security controls.
11.7 Discarding Electronic Media. Institutions must discard Electronic Devices and Media containing University Data:

(a) in a manner that adequately protects the confidentiality of the Data and renders it unrecoverable, such as overwriting or modifying the Electronic Media to make it unreadable or indecipherable or otherwise physically destroying the Electronic Media; and

(b) in accordance with the applicable institutional records retention schedule.
12.1 Reporting Requirements. Security Incidents will be reported as required by State and Federal law and University Policy including the U. T. System Information Security Incident Reporting Requirements.

12.2 Incident Management Procedures. All Institutions must adopt Incident Management Procedures to ensure that each Security Incident is reported, documented, and resolved in a manner that meets legal requirements and restores operations quickly. Incident Management must incorporate Procedures for:

(a) formally identifying, classifying, and reporting Security Incidents;
(b) responding to Security Incidents;
(c) assessing potential damage of Security Incidents;
(d) gathering and preserving physical and electronic evidence;
(e) assigning responsibility for gathering, maintaining, and reporting detailed Information regarding Security Incidents of local and U. T. Systemwide significance; for actions taken to remediate; and for documentation of a management action plan to prevent a recurrence;
(f) notifying appropriate Institutional and U. T. System officials, residents of Texas, Data Owners, Federal and State agencies, and consumer reporting agencies as required by applicable State and Federal law and U. T. System Policy;
(g) determining and adhering to timing requirements for incident disclosure and notification; and
(h) determining and adhering to an appropriate medium to provide notice based on incident significance, number of individuals adversely impacted, University Policy, applicable Federal and State law and regulations, and any contractual obligations with third-party organizations.

12.3 Employee Reporting. All employees must promptly report unauthorized or inappropriate disclosure of Confidential Data, in digital, paper, or any other format, to their supervisors and the Institutional Information Security Office.

12.4 Reporting to the Institutional Information Security Officer. Information Resources Owners, Custodians, and any supervisor or manager who
becomes aware of a Security Incident is to report the incident to the Institutional Information Security Officer.

12.5 Reporting Requirements to U. T. System. ISOs must report significant Security Incidents, as defined by the U. T. System Security Incident Reporting Requirements, to the U. T. System CISO. Security Incidents resulting in unauthorized disclosure of University Data must be reported immediately. ISOs must report Security Incidents to the U. T. System CISO prior to reporting to non-U. T. System agencies or organizations except as required by State or Federal law.

12.6 Monitoring Techniques and Procedures. Custodians must implement monitoring controls and Procedures for detecting, reporting, and investigating incidents.

U. T. System recognizes the special Risks associated with the collection, use, and disclosure of all or part of a social security number. Accordingly, the requirements of this Standard apply to all or part of a social security number contained in any medium, including paper records, that are collected, maintained, used, or disclosed by any Institution except UTIMCO.

13.1 All Institutions shall reduce the use and collection of social security numbers.

(a) All Institutions shall discontinue the use of all or part of the social security number as an individual’s primary identification number unless required or permitted by law. The social security number may be stored as a confidential attribute associated with an individual only if use of the social security number is essential for the performance of a mission related duty.

(b) If the maintenance and use of social security numbers is permitted, but not required by applicable law, the Institution shall permit the maintenance and use of social security numbers only as reasonably necessary for the proper administration or accomplishment of their respective business, governmental, educational and medical purposes and only if the Institution determines that the necessity outweighs the potential Risk created by the particular maintenance or use of the social security number. Potential purpose may include:

i. use as a means of identifying an individual for whom a unique identification number is not known;

ii. use for internal verification or administrative purposes where it is not feasible to use some other identifier; and

iii. use for verification or administrative purposes by a third-party or its agent in conducting the Institution’s business on behalf of the Institution where the third-party or agent has contracted to comply with the safeguards described in UTS165 Standard 11 - Safeguarding Data.

(c) Except in those instances in which an Institution is legally required to collect a social security number, an individual shall not be required to disclose all or part of his or her social security number, nor shall the individual be denied access to the services at issue if the individual refuses to disclose his or her social security number. An individual, however, may volunteer his or her social security number. An Institution’s request that an individual provide his or her
social security number for verification of the individual's identity
where the social security number has already been disclosed does
not constitute a disclosure for purposes of this Standard. The links
include examples of Federal laws and State laws that require the
collection or use of social security numbers. Questions about
whether a particular use is required by law should be directed to the
local Information Security Officer who will consult with the Office of
General Counsel with respect to the interpretation of law.

(d) An Institution may, but is not required to, designate only selected
offices and positions as authorized to request that an individual
disclose his or her social security number.

(e) All Institutions shall assign a unique identifier for each applicant,
student, employee, insured dependent, research subject, patient,
alumnus, donor, contractor, and other individuals, as applicable, at
the earliest possible point of contact between the individual and the
Institution for use in lieu of a social security number.

(f) The unique identifier shall be used in all electronic and paper
Information Systems to identify, track, and serve these individuals.
The unique identifier shall:

i. be a component of a system that provides a mechanism for the
   public identification of individuals;

ii. be permanent and unique within the Institution as applicable,
    and remain the property of, and subject to the rules of, that
    Institution; and

iii. not be derived from the social security number of the individual;
    or, in the alternative, if the unique identifier is derived from the
    social security number, it must be computationally infeasible to
    ascertain the social security number from the corresponding
    unique identifier.

(g) All services and Information Systems shall rely on the identification
services provided by the unique identifier system.

13.2 All Institutions shall provide notice to individuals when they collect social
security numbers.

(a) Each time an Institution requests that an individual initially disclose
his or her social security number, it shall provide the notice required
by Section 7 of the Federal Privacy Act of 1974 (5 U.S.C. § 552a),
which requires that the individual be informed whether the
disclosure is mandatory or voluntary, by what statutory or other
The University of Texas System
Information Resources Use and Security Policy
Policy: UTS165

authority the number is solicited, and what uses will be made of it. A subsequent request for production of a social security number for verification purposes does not require the provision of another notice.

i. The notice shall use the applicable text from Preapproved Sample Disclosures or such other text as may be approved by the Institution’s legal office or Office of General Counsel.

ii. Notices shall be in writing if possible. If a verbal notice is required, such notice shall be promptly documented.

(b) In addition to the notice required by the Federal Privacy Act, when the social security number is collected by means of a form completed and filed by the individual, whether the form is printed or electronic, the notice as required by Section 559.003 of the Texas Government Code must also be provided. That section requires that the agency state on the paper form or prominently post on the Internet site in connection with the form that: with few exceptions, the individual is entitled on request to be informed about the information that is collected about the individual; under Sections 552.021 and 552.023 of the Government Code, the individual is entitled to receive and review the information; and under Section 559.004 of the Government Code, the individual is entitled to have the incorrect information about the individual corrected.

(c) Employees may not seek out or use social security numbers relating to others for their own interest or advantage.

(d) All Institutions shall eliminate the public display of social security numbers.

i. Grades may not be publicly posted or displayed in a manner in which all or any portion of either the social security number or the unique identifier identifies the individual associated with the information.

ii. Social security numbers shall not be displayed on documents that are accessible to individuals who do not have a business reason to access the numbers. This section does not prohibit the inclusion of the social security number on transcripts or on materials for Federal or State Data reporting requirements.

iii. If an Institution must send materials containing social security numbers through the mail, the social security number must be placed in an envelope in such a way that ensures that no part of the social security number is visible from the outside.
iv. The Institution shall prohibit employees from sending social security numbers over the Internet or by email unless the connection is secure or the social security number is encrypted or otherwise secured. The Institution shall require employees sending social security numbers by fax to take appropriate measures to protect the confidentiality of the fax (such measures may include confirming with the recipient that the recipient is monitoring the fax machine).

v. The Institution shall not print or permit a third-party acting on behalf of the Institution to require that an individual's social security number be printed on a card or other device required to access a product or service provided by, on behalf of, or through the Institution.

13.3 All Information Systems acquired or developed must comply with the following:

(a) the Information System must use the social security number only as a Data element or alternate key to a database and not as a primary key to a database;

(b) the Information System must not display social security numbers visually (such as on monitors, printed forms, system outputs) unless required or permitted by law or permitted by this Standard;

(c) name and directory systems must be capable of being indexed or keyed on the unique identifier, once it is assigned, and not on the social security number; and

(d) for those databases that require social security numbers, the databases may automatically cross-reference between the social security number and other Information through the use of conversion tables within the Information System or other technical mechanisms.
UTS165 Standard 14: Information Services (IS) Privacy.

Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University have no expectation of privacy regarding any University Data they create, send, receive, or store on University-owned computers, Servers, or other Information Resources owned by, or held on behalf of, the University. The University may access and monitor its Information Resources for any purpose consistent with the University’s duties and/or mission without notice.
15.1 Procedures. In order to preserve the security of U. T. System Information Resources and Data, Strong Passwords must be used to control access to Information Resources. All Passwords must be constructed, implemented, and maintained according to the requirements of the U. T. System Identity Management Federation Member Operating Practices (MOP) and applicable Policies, Standards, and/or Procedures governing Password management. Institutional Policies, Standards, and/or Procedures must incorporate processes for:

(a) ensuring User identity when issuing or resetting a Password;
(b) establishing and enforcing Password strength;
(c) changing Passwords;
(d) managing security tokens when applicable;
(e) securing unattended Computing Devices from unauthorized access by implementing mechanisms to prevent password guessing (e.g., lockout after multiple login attempts) and to block access to idle sessions (e.g., a password-protected locking screen saver, session time-outs); and
(f) ensuring that Passwords are only accessed by or visible to the authenticating User, device, or system.

15.2 Sharing. Users must not share Passwords or similar Information, or devices used for identification and authorization purposes.
UTS165 Standard 16: Data Center Security.

16.1 Protection. All Information Resources must be physically protected based on Risk.

16.2 Safeguards. All Institutions shall adopt safeguards to ensure appropriate granting, controlling, and monitoring of physical access. Physical access safeguards must incorporate Procedures for:

(a) protecting facilities in proportion to the criticality or importance of their function and the confidentiality of any Information Resources affected;

(b) managing access cards, badges, and/or keys;

(c) granting, changing, and/or removing physical access to facilities to reflect changes in an individual’s role or employment status; and

(d) controlling visitor and Vendor physical access with Procedures that incorporate the following:
   i. advanced scheduling, logging, and documenting of visits;
   ii. escorting while on premises; and
   iii. restricting the unauthorized use of photographic and video devices while on premises.

16.3 Central IT Managed Data Centers and U. T. System Shared Data Centers. In addition to the controls required in Standard 16.2, Data Centers managed by Institutional Central IT organizations and the U. T. System Shared Data Centers must incorporate procedures for each of the following:

(a) reviewing physical access at least monthly, or more often if warranted by Risk;

(b) designating staff who will have authorized access during an emergency;

(c) monitoring the exterior and interior of the facility 24/7 by trained staff;

(d) maintaining appropriate environmental controls such as alarms that monitor heat and humidity, fire suppression and detection systems supported by an independent energy source, and uninterruptable power systems capable of supporting all Computing Devices in the event of a primary power system failure; and
(e) protecting any Shared or Central IT managed Data Center built after the effective date of this Standard by implementing and maintaining the following:

    i. security fencing, lighting, and landscaping to prevent concealment of intruders;

    ii. electronic alarms for all entry points into the facility and any internal areas housing critical infrastructure; and

    iii. computer rooms with no externally facing windows.

16.4 Decentralized IT Managed Data Centers. In addition to the controls required in Standard 16.2, the ISO shall develop Institutional Standards and safeguards to protect Decentralized IT Data Centers based on Risk.
UTS165 Standard 17: Security Monitoring.

17.1 At minimum, the Institutional Information Security Officer must ensure:

(a) that network traffic and use of Information Resources is monitored as authorized by applicable law and only for purposes of fulfilling a System or Institutional mission related duty;

(b) Server and network logs are reviewed manually or through automated processes on a scheduled basis based on Risk and regulation to ensure that Information Resources containing Confidential Data are not being inappropriately accessed;

(c) vulnerability assessments are performed annually, at minimum, to identify software and configuration weaknesses within information systems maintained in both Centralized and Decentralized IT;

(d) an annual, professionally administered and reported external network penetration test is performed; and

(e) that results of log reviews, vulnerability assessments, penetration tests, and IT audits are available to the ISO and that required remediation is implemented.

18.1 Initial and Recurring Training. The Institutional ISO shall ensure that security training is delivered and tracked. Initial and recurring training:

(a) should, at minimum, identify User responsibilities, common threats, regulatory and Institutional requirements regarding the acceptable use and security of Information Resources, proper handling of Confidential Data, and incident notification; and

(b) is to be administered in accordance with the following schedule, or more frequently as determined by an Institution.

i. Each new, temporary, contract, assigned, or engaged employee or worker must complete initial training within 30 days after the date that such a person is hired by the Institution or otherwise engaged or assigned to perform such work.

ii. Recurring training for employees and workers with access to Institutional Information Resources shall take place at least every two years.

18.2 In addition to initial training, Owners and Custodians should receive periodic training addressing the responsibilities associated with their roles. Method of delivery and scheduling of such training should be determined by the ISO.

18.3 Awareness Training should, at minimum, identify common threats, proper handling of Confidential Data, behaviors that increase Risk, behaviors that reduce Risk, and incident notification. Method of delivery and scheduling of awareness training should be determined by the Institutional ISO.

18.4 Technical Support Training. Owners and Custodians must provide, based on role, appropriate technical training equivalent to current industry standards for Information Security Administrators and employees providing Information Technology help-desk or technical support for Information Resources under their authority.
UTS165 Standard 19: Server and Device Configuration and Management.

19.1 Network Infrastructure Configuration. All Institutions must designate responsibility for the Institutional Network Infrastructure and specify those responsible for:

(a) configuring and managing the resource in accordance with U. T. System and Institutional information security Policies, Standards, and Procedures by:

i. segmenting the Institutional network either physically or logically to reduce the scope of exposure of Information Resources commensurate with the Risk and value of the Information Resource and Data; and

ii. separating Internet-facing applications from internal applications;

(b) maintaining appropriate access to the Network Infrastructure in accordance with U. T. System and Institutional information security Policies, Standards, and Procedures; and

(c) managing, testing, and installing updates to operating systems and applications for network equipment under their responsibility.

19.2 Server Hardening. To protect against malicious attack, all Servers on U. T. System networks will be security hardened based on Risk and must be administered according to Policies, Standards, and Procedures prescribed by the Institution, as applicable, and must incorporate Procedures for:

(a) identifying and assigning appropriately trained administrators for all Mission Critical Servers, or Servers supporting Information Systems containing Confidential Data;

(b) setting baseline security “hardened” configuration Standards for all Servers; and

(c) managing the testing and installation of service packs, hot fixes, and security patches.

19.3 Device Configuration. All devices (e.g., routers, laptops, tablets, desktops, and handheld devices) on U. T. System networks must be protected against malicious attack. The Institutional ISO shall establish and communicate security configurations based on Risk and incorporate Procedures for:

(a) setting baseline security “hardened” configuration Standards for all devices;
(b) establishing and making available minimum security configurations for University-owned and Non-University Owned Portable Computing Devices; and

(c) recommended patch management practices.

19.4 Device Management. The Institutional ISO shall ensure that devices are administered by professionally trained staff in accordance with Policies, Standards, and Procedures prescribed by the Institution.

19.5 Access to Information Security Information and Devices. All Owners and Custodians of University owned, leased, or controlled Information Resources must provide the Institutional ISO with direct access to detailed security status information including, but not restricted to the following: firewall rules, IPS/IDS rules, security configurations and patch status; and sufficient access rights to Servers and devices to independently and effectively execute Institutional ISO monitoring duties.
UTS165 Standard 20: Software Licensing.

Software is to be used in accordance with the applicable licensing agreement. Unauthorized or unlicensed use of software is prohibited and subjects the User to disciplinary action. Any unauthorized or unlicensed use is deemed to be without the consent of U. T. System.

21.1 Information Security Consideration. All Institutions must adopt Institutional Policies, Standards and/or Procedures to ensure that the protection of Information Resources (including Data confidentiality, integrity, and availability) is considered during the development or purchase of new Information Systems or services.

21.2 Redundant Information Systems or Services. Information Systems that duplicate services provided by the Institution’s Central IT organization are discouraged because they increase opportunity for exposure of Data. The Information Resources Manager shall approve the purchase or deployment of new Decentralized IT Information Systems or services (e.g., electronic mail/web/file servers, file/system backup, storage, etc.) that duplicate applications or services provided by Centralized IT. The Owner of the duplicative Information System and the IRM must document and justify exceptions based on business need, weighed against Risk of unauthorized access or loss of Data.

21.3 Required Controls. The Institutional ISO shall develop institutional Policies, Standards, and/or Procedures that address the following:

(a) providing methods for appropriately restricting privileges of authorized Users to all production systems, applications, Data, and University-owned devices. User access to applications is granted on a need-to-access basis;

(b) maintaining separate production and development environments to ensure the security and reliability of the production system;

(c) performing a security assessment prior to the purchase of any new information security services that receive, maintain, and/or share Confidential Data;

(d) including vulnerability assessments and code scans to the Information Systems development cycle; and

(e) performing a vulnerability assessment and including a static or dynamic code scan of all new web applications prior to moving them to production.

21.4 Security Review and Approval. The Institutional ISO must review and approve security requirements, specifications, and, if applicable, third-party Risk assessments for any new computer hardware, software, applications, or services that are Mission Critical or that receive, maintain, and/or share Confidential Data.
21.5 IT Systems Contracts. Contracts for purchase or development of automated systems must address security, backup, and privacy requirements, and should include right-to-audit and other provisions to provide appropriate assurances that applications and Data will be adequately protected.

The U. T. System recognizes that Vendors and other contractors serve an important function in the development and/or support of services, hardware, and software and, in some cases, the operation of computer networks, Servers, and/or applications. This standard applies to contracts entered into by U. T. System or an Institution that involves third-party access to or creation of Information Resources or University Data by a third-party.

22.1 Contracts. Contracts of any kind, including purchase orders, memoranda of understanding (MOU), letters of agreement, or any other type of legally binding agreement, that involve current or future third-party access to or creation of Information Resources and/or Data must include terms determined by the Office of General Counsel as sufficient to ensure that Vendors and any subcontractors or other third-parties that maintain, create, or access University Data as the result of the contract comply with all applicable Federal and State security and privacy laws, this UTS 165, and any applicable U. T. System and University Policies or Standards, and must contain terms that ensure that all University Data affected by the contract is maintained in accordance with those standards at all times, including post-termination of the contract.

22.2 The Data Owner, Institutional procurement officers and staff, and the ISO are jointly and separately responsible for ensuring that all contracts are reviewed to determine whether the contract involves third-party access to, outsourcing, maintenance, or creation of University Data; and that all such access, outsourcing, or maintenance fully complies with this Standard at all times.

22.3 Any contract involving third-party access to, creation, or maintenance of Protected Health Information (PHI) as defined in 45 C.F.R. § 164.501, must include a Health Insurance Portability and Accountability Act (HIPAA) business associate agreement in a form approved by Institutional counsel or OGC.

22.4 Any contract involving third-party-provided credit card services must require that the Contractor provides assurances that all subcontractors who provide credit card services pursuant to the contract will comply with the requirements of the Payment Card Industry Data Security Standard (PCI DSS) in the provision of the services.

22.5 Vendor or other Third-Party Assessment. Prior to access, maintenance, or creation of University Data by a Vendor or any other third-party, the Institution must ensure that an assessment is or has been performed that is designed to ensure that:
(a) the Vendor has sufficient technological, administrative, and physical safeguards to ensure the confidentiality, security, and integrity of the Data at rest and during any transmission or transfer; and
(b) any subcontractor or other third-party that will access, maintain, or create Data pursuant to the contract will also ensure the confidentiality, security, and integrity of such Data while it is at rest and during any transmission or transfer.

22.6 As part of the Institution’s assessment of a Vendor or other third-party, the Institution will request copies of any self-assessments or third-party assessments that the Vendor or third-party has access to.

22.7 Access Control Measures. Each Institution must control Vendor and other third-party access to its Data based on Data sensitivity and Risk. Controls must incorporate the following:

(a) Vendor must represent, warrant, and certify it will:

i. hold all Confidential Data in the strictest confidence;

ii. not release any Confidential Data unless Vendor obtains Institution’s prior written approval and performs such a release in full compliance with all applicable privacy laws, including the Family Educational Rights and Privacy Act (FERPA);

iii. not otherwise use or disclose Confidential Data except as required or permitted by law;

iv. safeguard Data according to all commercially reasonable administrative, physical, and technical Standards (e.g., such Standards established by the National Institute of Standards and Technology or the Center for Internet Security);

v. continually monitor its operations and take any action necessary to assure the Data is safeguarded in accordance with the terms of UTS165 Policy and Standards; and

vi. comply with the Vendor access requirements that are set forth in this Standard.

22.8 Breach Notification. Institutions shall require the following from the Vendor.

(a) If an unauthorized use or disclosure of any Confidential Data occurs, the Vendor must provide:
i. written notice within one business day, or if The Data Owner, Institutional procurement officers, and the ISO are satisfied that a longer period is acceptable, within that period, after Vendor’s or third-party’s discovery of such use or disclosure; and

ii. all Information U. T. System requests concerning such unauthorized use or disclosure.

22.9 Return of Data. Within 30 days after the termination or expiration of a purchase order, contract, or agreement for any reason, Vendor must either:

(a) return or securely destroy, as specified by contract or agreement, all Data provided to the Vendor by the Institution, including all Confidential Data provided to Vendor’s employees, subcontractors, agents, or other affiliated persons or Institutions; or

(b) in the event that returning or securely destroying the Data is infeasible, provide notification of the conditions that make return or destruction infeasible, in which case the Vendor or third-party must:

i. continue to protect all Data that it retains;

ii. agree to limit further uses and disclosures of such Data to those purposes that make the return or destruction infeasible for as long as Vendor or other third-party maintains such Data; and

iii. to the extent possible, de-identify such Data.

23.1 Exception to an otherwise required security control may be granted by the Institutional ISO to address specific circumstances or business needs relating to an individual program or department only as authorized by applicable law, and System and Institutional Policy. Requests for exceptions of this type should be in writing and should be initiated by the Data Owner. Both the Institutional ISO and Data Owner are jointly responsible for ensuring that any exception is not contrary to applicable law.

23.2 The Information Security Officer may issue blanket exceptions to address Institution-wide situations.

23.3 All exceptions must be based on an assessment of business requirements weighed against the likelihood of an unauthorized exposure, and the potential adverse consequences for individuals, other organizations, or the Institution were an exposure to occur.

23.4 As a condition for granting an exception, the Institution ISO may require compensating controls be implemented to offset the risk.

23.5 All exceptions must be documented, and must include the following elements:

   (a) a statement defining the nature and scope of the exception in terms of the Data included and/or the class of devices included;
   
   (b) the rationale for granting the exception;
   
   (c) an expiration date for the exception;
   
   (d) a description of any compensating security measures that are to be required; and
   
   (e) acknowledgement, via signature (written, electronic, or through automated process), of the ISO, and, in the case of an exception resulting from a Data Owner request, of the Data Owner.

23.6 Encryption Exceptions.

   (a) The ISO may grant an exception to the use of encryption on a device if the ISO determines that encryption makes the device unsuitable to perform its intended functions and the Risk posed by the unencrypted device is minimal or moderate based on its use and/or other implemented compensating controls.
(b) The ISO may recommend to the Chief Administrative Officer an encryption exception be granted for a High Impact Device if encryption makes the device unsuitable to perform its intended function. Exception recommendations have the effect of being approved unless, upon review, the Chief Administrative Officer disapproves the recommendation.

23.7 A summary of exceptions and exception recommendations shall be reported to the President in the annual Presidential Information Security Program Report with sufficient detail to provide the President with an understanding of types of Risks and level of Institutional exposure.

Guidance for processing of laptop encryption exception requests is available at:
https://community.utsystem.edu/sites/infosec/Shared%20Documents%202/Encryption/Laptop%20Encryption%20FAQ%20Revision%207-1-2012.pdf

Guidance for processing of laptop encryption exception requests is available at:
https://community.utsystem.edu/sites/infosec/Shared%20Documents%202/Encryption/Desktop%20Encryption%20Requirements%20and%20FAQ.pdf

23.8 This standard does not apply to or authorize an Institutional ISO to grant exceptions to UTS165 Standard 2 – Acceptable Use of Information Resources.
UTS165 Standard 24: Disciplinary Actions.

Violation of this UTS 165 or other U. T. System or Institutional Information Security Policies or Standards by faculty, staff, and students who have access to U. T. System Information Resources or Data for the purpose of providing services to or on behalf of an Institution, are subject to disciplinary action in accordance with the applicable Institutional rules and Policies. For contractors and consultants, this may include termination of the work engagement and execution of penalties contained in the work contract. For interns and volunteers, this may include dismissal. Additionally, certain violations may result in civil action or referral for criminal prosecution.