



UT System Administration Policy Library -- Policy UTS165

UT System Information Resources Use and Security Policy

Responsible Officer: Chief Information Security Officer
Sponsoring Office: Office of the Chief Information Security Officer
Effective Date: April 12, 2007
Last Reviewed: January 5, 2010
Next Scheduled Review: June 15, 2010
Errors or changes to: policyoffice@utsystem.edu

CONTENTS

Policy Statement

Rationale

Scope

Website Address For This Policy

Related Statutes, Policies, Requirements Or Standards

Contacts

Definitions

Responsibilities

Procedures

Special Requirements for Initial Implementation of Policy

Forms Tools/Online Processes

Appendix

POLICY STATEMENT

It is the policy of The University of Texas System (UT System) to:

1. Protect Information Resources based on risk against accidental or unauthorized access, disclosure, modification, or destruction and assure the availability, confidentiality, and integrity of Data;
2. Appropriately reduce the collection, use or disclosure of social security numbers contained in any medium, including paper records;
3. Apply appropriate physical and technical safeguards without creating unjustified obstacles to the conduct of the business and Research of the UT System and the provision of services to its many constituencies in compliance with applicable state and federal laws.

RATIONALE

Title 1 Texas Administrative Code 202.70 (1) states that it is the policy of the state of Texas that Information Resources residing in the various institutions of higher education of state government are strategic and vital assets belonging to the people of Texas. Assets of UT System must be available and protected commensurate with their value and must be administered in conformance with federal and state law and The University of Texas System *Regents' Rules and Regulations*. This Policy provides requirements and guidelines to establish accountability and prudent and acceptable practices regarding the use and safeguarding of the UT System Information Resources; protect the privacy of personally identifiable information contained in the Data that constitutes part of its Information Resources; ensure compliance with applicable policies and state and federal laws regarding the management and security of Information Resources; and, educate individual Users with respect to the responsibilities associated with use of UT System Information Resources.

This policy, which includes appended Information Security Practice Bulletins, is intended to serve as the foundation for each institution's, System Administration's and UTIMCO's (collectively known as "the Entities") computer security program, providing these Entities the authority to implement policies, practice standards, and/or procedures necessary to implement a successful Information Security Program in compliance with this policy.

Information that is collected pursuant or that is related to an Entity's Information Security Program is subject to Section 552.139 of the Texas Government Code and is therefore confidential by law. Accordingly, an Entity may not withhold information or fail to include information required by this Policy and/or Security Practice Bulletins to be provided to or included in an Entity's Information Security Program.

This Policy consolidates the following policies:

- UTS 165 Information Resources Use and Security Policy;
- UTS 166 Protecting the Confidentiality of Social Security Numbers; and
- UTS 167 Protecting the Confidentiality and Integrity of Digital Research Data

Most of the requirements in this policy were consolidated from three previous policies: UTS 165 (previously BPM 53) "Information Resources Use and Security Policy", UTS 167 (previously BPM 75) "Protecting the Confidentiality and Integrity of Digital Research Data", and UTS 166 (previously BPM 66) "Protecting the Confidentiality of Social Security Numbers. All of the requirements in this current policy apply to all UT System Data, including social security numbers that are maintained, transmitted, or made available in electronic media ("Digital Data"). However, the special requirements governing the use, disclosure and maintenance of social security numbers, now set forth in Section 10 of this policy, apply to social security numbers contained in *any* media, including paper records, held by all Entities except UTIMCO. Therefore, special caution should be exercised when collecting, using or disclosing any Data that includes a social security number.

SCOPE

All Entities

WEBSITE ADDRESS FOR THIS POLICY

<http://www.utsystem.edu/policy/policies/uts165.html>

RELATED STATUTES, POLICIES, REQUIREMENTS OR STANDARDS

UT System Administration Policies & Standards	Other Statutes, Policies & Standards
	<ul style="list-style-type: none"> • Title 1 <i>Texas Administrative Code</i> 202.2 • Texas Education Code § 65.31 • 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) • Family Educational Rights and Privacy Act, 20 U. S. C. § 1232g • Texas Business and Commerce Code §35.58 • Texas Government Code § 559.003

CONTACTS

If you have any questions about UT System Administration Policy UTS165 Information Resources Use and Security Policy, contact the following offices:

Subject	Office Name	Telephone Number	Email/URL
	Office of the Chief Information Security Officer	(512) 499-4249	ciso@utsystem.edu

DEFINITIONS

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system failure.

Change: Any addition, modification or update, or removal of an Information Resource that can potentially impact the operation, stability, or reliability of an Entity network or computing environment.

Change Management: Process of controlling the communication, approval, implementation, and documentation of modifications to hardware and software 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 Entity. For most Entities, this is the President.

Computer Virus: A computer program that attaches itself to a file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive without the knowledge or permission of the User. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows Users to generate macros.

Confidential Data: Data that is exempt from disclosure under the provisions of the Public Records Act or other applicable state and federal laws.

Confidential University Data: Confidential Data maintained by an Entity of The University of Texas System.

Custodian: An individual or entity responsible for implementing Owner-defined controls and access to an Information Resource. Custodians include Information Security Administrators, Entity information technology/systems departments, vendors, and any third party acting as an agent of or otherwise on behalf of an Entity.

Data: Recorded data, regardless of form or media in which it may be recorded, which constitute the original data necessary to support the business of UT System or original observations and methods of a study and the analyses of such original data that are necessary to support Research activities and validate Research findings. Data may include but is not limited to: printed records, observations and notes; electronic data; video and audio records, photographs and negatives, etc.

Decentralized Areas: Entity 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 or maintained made available in, electronic media.

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, and other paperless means of communication.

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

Electronic Media: Any of the following: a) 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 b) 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.

Email: Abbreviation for Electronic Mail.

Entity or Entities: The nine academic teaching institutions and the six health science centers in The University of Texas System, UT System Administration, and UTIMCO.

Information: Data organized, formatted and presented in a way that facilitates decision making. All information is data.

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

Information Resources Manager (IRM): The IRM is responsible for management of all of the Entity's information resources. The designation of an Entity information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the Entity's information activities, and ensure greater visibility of such activities within and between Entities. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the Entity including both central and decentralized areas. If an Entity does not designate an IRM, the title defaults to the institution's president, and the president is responsible for adhering to the duties and requirements of an IRM.

Information Security Program: The policies, procedures, elements, structure, strategies, plans, metrics, reports, and resources that establish an information resources security function within an Entity.

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, information, data, applications, communications and people.

Integrity: The accuracy and completeness of information and assets and the authenticity of transactions.

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

Lead Researcher: The person engaged in the conduct of Research with primary responsibility for stewardship of Research Data on behalf of an Entity.

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.

Mission Critical Information Resources: Information Resources defined by an Entity to be essential to the Entity's function and which if made unavailable will inflict substantial harm to the Entity and the Entity's ability to meet its instructional, research, patient care, or public service missions. Mission Critical Information Resources include Confidential Data.

Non-University Owned Computing Device: Any device that is capable of receiving, transmitting, and/or storing electronic data and that is not owned or leased by or under the management of an Entity.

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.

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

Personal Identifying Information: Information that alone or in conjunction with other information identifies an individual, including an individual's name, social security number, date of birth, or government-issued identification number; mother's maiden name; unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; unique electronic identification number, address, or routing code; and telecommunication access device.

Portable Computing Devices: Any easily portable device that is capable of receiving, transmitting, and/or storing data. These include, but are not limited to, notebook computers, handheld computers, PDAs (personal digital assistants), pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs and similar storage devices.

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.

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

Security Incident: An event which results in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.

Sensitive Data: Digital Data maintained by an Entity that requires higher than normal security measures to protect it from unauthorized access, modification or deletion. Sensitive Data may be either public or confidential and is defined by each Entity based on compliance with applicable federal or state law or on the demonstrated need to (a) document the integrity of that Digital Data (i.e., that the Data had not been altered by either intent or accident), (b) restrict and document individuals with access to that Digital Data, and (c) ensure appropriate backup and retention of that Digital Data. These would most frequently be required by:

- Federal agencies (e.g., Food and Drug Administration);

- State agencies (e.g., data defined as High-Risk Information Resources by 1 TAC 202.72);
- Employee benefit providers;
- Office of General Counsel or Entity Office of Legal Affairs (i.e. data subject to or involved in litigation or confidentiality agreements);
- Intellectual Property and /or Technology Transfer requirements; or
- Federal regulations (e.g., FERPA, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, Biodefense, Homeland Security, DOD etc.)

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

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

User: An individual, automated application or process that is authorized by the Owner to access the resource, in accordance with the Owner's procedures and rules. Has the responsibility to (1) use the resource only for the purpose specified by the Owner, (2) comply with controls established by the Owner, and (3) prevent disclosure of Confidential or Sensitive 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 UT System's investment assets.

UT System Administration: The central administrative offices that lead and serve the Entities by undertaking certain central responsibilities that result in greater efficiency or higher quality than could be achieved by individual Entities or that fulfill legal requirements.

Vendor: Someone outside of UT System who exchanges goods or services for money or other consideration.

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

RESPONSIBILITIES

Chancellor

- Budgets sufficient resources to fund ongoing and continuous information security remediation, implementation and compliance activities that reduce compliance risk to an acceptably low level.
- Ensures that appropriate corrective and disciplinary action is taken in the event of non-compliance.

Chief Administrative Officer

- Ensures the Entity's compliance with this Policy.
- Budgets sufficient resources to fund ongoing and continuous information security remediation, implementation and compliance activities (e.g., staffing, training, tools, and monitoring activities) that reduce compliance risk to an acceptably low level.
- Approves the Entity Information Security Program, or designate someone to provide this approval in accordance with 1 TAC 202.71(a).
- Ensures that appropriate corrective and disciplinary action is taken in the event of non-compliance.
- Designates an individual other than the Information Resources Manager to serve as the Information Security Officer (ISO) who shall serve in the capacity as required by 1 TAC 202.71(d) and with authority for that entire Entity.

Chief Information Security Officer (for UT System)

- Provides leadership, strategic direction, and coordination for the UT System-wide information security initiative including issuing [security practice bulletins](#) relating to standards and best practices.
- Establishes the UT System CISO Council and holds meetings at least quarterly.
- Develops and provides oversight for a UT System-wide Information Security Compliance Program.
- Provides guidance on the Entity Information Security Program including organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum standards.
- Defines the risk management process to be used for all information security risk management activities.
- Explores and recommends the acquisition of tools and resources that can be utilized UT System-wide and how expertise can be shared among Entities.
- Establishes reporting guidance, metrics, and timelines and monitors effectiveness of security strategies at each Entity.

- Apprises the Chancellor and the Board of Regents quarterly on the status and effectiveness of the Information Security Compliance Programs and activities at each Entity.

Custodian of Mission Critical Information Resources

- Implements approved mitigation strategies and adhere to information security policies and procedures to manage risk levels for information resources under their care.
- Implements monitoring techniques and procedures for detecting, reporting, and investigating incidents.

Department Head and/or Lead Researcher

- Comply with this Policy as it relates to Non-Research and Research Data respectively under their control including when holding subcontracts for projects in which the prime award is at another institution or agency.

Entity

- Designates responsibility for the information security function by documenting key roles and responsibilities.
- Adopts change management processes to ensure secure, reliable, and stable operations to which all offices that support Information Resources are required to adhere.
- Performs annual risk assessments that identify Mission Critical Information Resources in the central and all decentralized areas.
- Develops Digital Data classification guidelines for Digital Data maintained in both central and decentralized areas.
- Develops a plan for identifying Digital Data that is Sensitive.
- Manages and protects the confidentiality and integrity of Sensitive Digital Data.
- Controls and monitors access to its Sensitive Digital Data based on data sensitivity and risk.
- Discontinues use of social security number as an individual's primary identification number.
- Uses and collects social security numbers only as reasonably necessary for the proper administration or accomplishment of the Entity's business, governmental, educational and medical purposes.
- Assigns a unique identifier for each applicant, student, employee, insured dependent, research subject, patient, alumnus, donor, contractor, and other individuals who become associated with the Entity at the earliest possible point of contact with the Entity.

- Provides the notice required by Section 7 of the Federal Privacy Act of 1974 and by Section 559.003 of the Texas Government Code each time it requests that an individual initially disclose his or her social security number.
- Limits and monitors access to records containing social security numbers to those employees who need to see the number for the performance of the employees' job responsibilities.
- Follows procedures to report incidents involving computer security, as required by state or federal law.
- Reports significant information security incidents, as defined by the [UT System Security Incident Reporting Guidelines](#), to the UT System CISO.
- Discloses in accordance with applicable federal and state law, incidents involving computer security that compromises the security, confidentiality, or integrity of Personal Identifying Information it maintains to any resident of Texas and Data Owners whose Personal Identifying Information was, or is reasonably believed to have been, acquired without authorization.
- Adheres to policies, standards and/or procedures governing the secure transmission of Confidential University Data via public networks.
- Provides computer security awareness training.
- Ensures that the protection of Information Resources (including data confidentiality, integrity, and accessibility) is considered during the development or purchase of new computer applications.
- Ensures that information technology contracts address security, backup and privacy requirements, and include right-to-audit or other provisions to provide appropriate assurances that applications and Data will be adequately protected.
- Monitors Information Resources in accordance with TAC 202.75 (7) (P).

Entity Offices with Designated Responsibility For Network and/or Application Account Creation

- Manages accounts in accordance with the Entity's information security policies, standards, and/or procedures.
- Approves all access methods, installation of all network hardware connected to the local-area network and methods and requirements for attachment of any non UT System owned computer systems or devices to the UT System network.

Entity Office Charged With Supporting Information Resources

- Formalizes best practice change management processes into practice standards.
- Requires compliance from all individuals who manage Information Systems or applications.
- Provides support, guidance and problem resolution to department heads and Lead Researchers with respect to this Policy and applicable policies and procedures.

Information Security Administrator

- Implements and complies with all information technology policies and procedures relating to assigned systems.
- Assists Owners in performing annual information security risk assessment for Mission Critical Resources.
- Reports general computing and Security Incidents to the Entity ISO.
- Assists, as member of the ISA Work Group, the ISO in developing, implementing, and monitoring the Information Security Program.
- Establishes reporting guidance, metrics, and timelines for ISOs to monitor effectiveness of security strategies implemented in both the central and decentralized areas.
- Reports at least annually to the ISO about the status and effectiveness of information resources security controls.

Information Security Officer (at each Entity)

- Provides information security for all Information Systems and computer equipment maintained in both central and decentralized areas.
- Develops a full-scale Entity Information Security Program.
- Documents an information security risk assessment annually that identifies Mission Critical Information Resources in the central and all decentralized areas.
- Ensures an annual information security risk assessment is performed by each Owner of Mission Critical Information Resources.
- Requires each Owner of Mission Critical Information Resources to designate an Information Security Administrator (ISA).
- Establishes an Entity Information Security Working Group composed of ISAs and holds meetings at least quarterly.
- Documents and maintains up to date an Entity Information Security Program.
- Establishes reporting guidance, metrics, and timelines and monitors effectiveness of security strategies in both central and decentralized operations.
- Specifies and requires use of appropriate security software such as anti-virus, firewall, configuration management, and other security related software on computing devices owned, leased, or under the custodianship of any department, operating unit, or an individual who is serving in the role as an employee of the Entity as deemed necessary by the ISO to provide appropriate information security across the whole of the Entity.
- Ensures that high-level information security awareness training is included in first-time Compliance Training and in every subsequent update for all employees.
- Ensures that ISAs and Data Owners are properly trained on information security requirements.

- Communicates instances of non-compliance to appropriate administrative officers for corrective, restorative and/or disciplinary action.
- Participates in the UT System CISO Council meetings.
- Reports quarterly to the UT System CISO the current status of the information security risk assessment and Information Security Program, including any significant incidents, situations of non-compliance, barriers to program execution, and planned remedies for the whole Entity.
- Reports, at least annually, to the Chief Administrative Officer or his or her designated representative(s) and copies to the Entity's Chief Information Officer and Compliance Officer, and the System-wide Chief Information Security Officer on the status and effectiveness of information resources security controls for the whole Entity.
- Reviews the data security requirements and specifications of any new computer applications or services that receive, maintain, and/or share Confidential Data.
- Approves the security requirements of the purchase of required information technology hardware, software, and systems development services.
- Approves and documents any exceptions to information security practices within the Entity.

Institutional Compliance and Internal Audit

- Provide high-level monitoring of the Information Security Program through inspections and verifications of reported information and periodic audits respectively.

Owner

- Grants access to the Information System under his/her responsibility.
- Classifies Digital Data based on Data sensitivity and risk.
- Backs up Data under his/her responsibility in accordance with risk management decisions and secures back up media.

Owner of Mission Critical Information Resources

- Designates an individual to serve as an Information Security Administrator (ISA) to implement information security policies and procedures and for reporting incidents to the ISO.
- Performs an annual information security risk assessment and identifies, recommends, and documents acceptable risk levels for information resources under his/her authority.

User Accessing UT System Information Resources

- Complies with this Policy.
- Formally acknowledges and abides by the Entity’s acceptable use policies.
- Does not share passwords or similar information or devices used for identification and authorization purposes.
- Adheres to prudent and responsible Internet use practices as outlined in the Entity’s policies associated with Information Resources acceptable use.

Vendor

- Adheres to all state and federal laws and Regents’ *Rules and Regulations* pertaining to the protection of Information Resources and privacy of Sensitive Data.
- Complies with all applicable UT System rules associated with this Policy, practice standards and agreements, and adheres to federal and state laws to which UT System must adhere.
- Represents, warrants, and certifies it will hold all UT System Sensitive Data in the strictest confidence.

PROCEDURES

1. Information Resources Security Responsibility and Accountability

1.1 All Entities must designate responsibility for the information security function by documenting key roles and responsibilities.

1.2 The Chancellor shall be responsible for the following:

1.2.1 Budget sufficient resources to fund ongoing and continuous information security remediation, implementation and compliance activities that reduce compliance risk to an acceptably low level; and

1.2.2 Ensure that appropriate corrective and disciplinary action is taken in the event of non-compliance.

1.3 The Chief Administrative Officers at each Entity shall be responsible for the following:

1.3.1 The Entity’s compliance with this Policy;

1.3.2 Budget sufficient resources to fund ongoing and continuous information security remediation, implementation and compliance activities (e.g., staffing, training, tools, and monitoring activities) that reduce compliance risk to an acceptably low level;

1.3.3 Approve the Entity Information Security Program, or designate someone to provide this approval in accordance with 1 TAC 202.71(a); and

1.3.4 Ensure that appropriate corrective and disciplinary action is taken in the event of non-compliance.

1.4 The Chancellor shall designate an individual to serve as UT System Chief Information Security Officer (CISO). The responsibilities of the UT System CISO shall include the following:

1.4.1 Provide leadership, strategic direction, and coordination for the UT System-wide information security program including issuing [security practice bulletins](#) relating to standards and best practices;

1.4.2 Establish the UT System CISO Council and hold meetings at least quarterly;

1.4.3 Develop and provide oversight for a UT System-wide Information Security Compliance Program. This program shall include UT System-wide and Entity action plans, training plans, and monitoring plans;

1.4.4 Provide guidance on the Entity Information Security Program including organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum standards;

1.4.5 Define the risk management process to be used for all information security risk management activities;

1.4.6 Explore and recommend the acquisition of tools and resources that can be utilized UT System-wide and how expertise can be shared among Entities;

1.4.7 Establish reporting guidance, metrics, and timelines and monitor effectiveness of security strategies at each Entity; and

1.4.8 Apprise the Chancellor and the Board of Regents quarterly on the status and effectiveness of the Information Security Compliance Programs and activities at each Entity.

1.5 The highest ranking administrator at each Entity charged with oversight of information technology at that Entity shall serve in the functional role of Information Resources Manager (IRM) as defined by 1 TAC 211.20 and will have authority for the entire Entity.

1.6 The Chief Administrative Officer at each Entity shall designate an individual other than the IRM to serve as the Information Security Officer (ISO) who shall serve in the capacity as required by 1 TAC 202.71(d) and with authority for that entire Entity. The responsibilities of the ISO shall include the following:

- 1.6.1 Provide information security for all Information Systems and computer equipment maintained in both central and decentralized areas;
- 1.6.2 Develop a full-scale Entity Information Security Program. This program shall include Entity action plans, training plans, and monitoring plans.
- 1.6.3 Document an information security risk assessment annually in accordance with 1 TAC 202.72 that identifies Mission Critical Information Resources in the central and all decentralized areas;
- 1.6.4 Ensure an annual information security risk assessment is performed (using the process defined above) by each Owner of Mission Critical Information Resources;
- 1.6.5 Require each Owner of Mission Critical Information Resources to designate an Information Security Administrator (ISA);
- 1.6.6 Establish an Entity Information Security Working Group composed of ISAs and hold meetings at least quarterly;
- 1.6.7 Document and maintain up to date an Entity Information Security Program. The Program shall identify specific mitigation strategies to be used by each Owner of Mission Critical Information Resources to manage identified risks;
- 1.6.8 Establish reporting guidance, metrics, and timelines and monitor effectiveness of security strategies implemented in both central and decentralized areas;
- 1.6.9 Specify and require use of appropriate security software such as anti-virus, firewall, configuration management, and other security related software on computing devices owned, leased, or under the custodianship of any department, operating unit, or an individual who is serving in the role as an employee of the Entity as deemed necessary to provide appropriate information security across the whole of the Entity
- 1.6.10 Ensure that high-level information security awareness training is included in first-time Compliance Training and in every subsequent update for all employees;
- 1.6.11 Ensure that ISAs and Data Owners are properly trained on information security requirements;
- 1.6.12 Communicate instances of non-compliance to appropriate administrative officers for corrective, restorative and/or disciplinary action;
- 1.6.13 Participate in the UT System CISO Council meetings;

1.6.14 Report quarterly to the UT System CISO the current status of the information security risk assessment and Information Security Program including any significant incidents, situations of non-compliance, barriers to program execution, and planned remedies for the whole Entity. The report is to include a certification that best efforts have been made to ensure appropriate strategies are in place to manage identified risks, that the strategies are being applied consistently over time, and that all Security Incidents have been reported; and

1.6.15 Report, at least annually, to the Chief Administrative Officer or his or her designated representative(s) and copied to the Entity's Chief Information Officer and Compliance Officer, and the System-wide Chief Information Security Officer on the status and effectiveness of information resources security controls for the whole Entity.

1.7 Owners of Mission Critical Information Resources at each Entity shall designate an individual to serve as an Information Security Administrator (ISA) to implement information security policies and procedures and for reporting incidents to the ISO. The responsibilities of the ISA shall include the following:

1.7.1 Implement and comply with all information technology policies and procedures relating to assigned systems;

1.7.2 Assists Owners in performing annual information security risk assessment for Mission Critical Resources.

1.7.3 Report general computing and Security Incidents to the Entity ISO;

1.7.4 Assist, as member of the ISA Work Group, the ISO in developing, implementing, and monitoring the Information Security Program;

1.7.5 Establish reporting guidance, metrics, and timelines for ISOs to monitor effectiveness of security strategies implemented in both the central and decentralized areas; and

1.7.6 Report at least annually to the ISO about the status and effectiveness of information resources security controls.

1.8 Department Heads and Lead Researchers at each Entity shall be responsible for compliance with this Policy as it relates to Non-Research and Research Data respectively under their control including when holding subcontracts for projects in which the prime award is at another institution or agency.

1.9 Institutional Compliance and Internal Audit at each Entity shall provide high-level monitoring of the Information Security Program through inspections and verifications of reported information and periodic audits respectively.

1.10 All Users must comply with this Policy. Users who fail to comply are subject to disciplinary action in accordance with Section 28.

2. Information Resources Acceptable Use

2.1 All Entities shall have an acceptable use policy. All individuals accessing UT System Information Resources must formally acknowledge and abide by the acceptable use policy. Formal acknowledgment of the Acceptable Use Policy by all individuals accessing UT System Information Resources serves as a compliance and enforcement tool.

2.2 Users are responsible for exercising good judgment regarding the reasonableness of personal use in accordance with all policies associated with Information Resources acceptable use.

2.3 As a convenience to the UT System User community, limited incidental personal use of Information Resources is permitted.

2.4 Incidental use of Information Resources must not result in direct cost to the UT System or expose UT System to unnecessary risks.

3. Account Management

The UT System recognizes that proper management and use of computer accounts are basic requirements for protecting UT System Information Resources. All Entities shall adopt Access Management processes to ensure that access is administered properly. All offices that create access accounts for network and/or applications are required to manage the accounts in accordance with such access management processes and the requirements of the UT System Identity Management Federation Member Operating Practices (MOP). Access to a system may not be granted by another User without the permission of the Owner or the Owner's delegate of that system. An Access Management Process must incorporate procedures for the following:

3.1 Creating uniquely identifiable accounts for all Users. This includes accounts created for use by outside vendors (see Section 26);

3.2 Reviewing, removing and/or disabling accounts at least annually, or more often if warranted by risk, to reflect current User needs or changes on User role or employment status; and

3.3 Expiring or disabling passwords at least annually or more often if warranted by risk.

4. Administrative/Special Access

All Entities shall adopt special procedures that ensure 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) shall be used only for their intended administrative purpose and that all authorized Users must be made aware of the responsibilities associated with the use of privileged special access accounts. These procedures must address:

- 4.1 Acceptable use of administrative/special access accounts and intended administrative purposes;
- 4.2 Authorizing use of administrative/special access accounts;
- 4.3 Reviewing, removing and/or disabling administrative/special access accounts at least annually, or more often if warranted by risk, to reflect current authorized User needs or changes on authorized User role or employment status; and
- 4.4 Escrowing login passwords for each secured system for access during emergencies. Individual User login passwords shall not be escrowed.

5. Backup Recovery of Network Servers and Data

5.1 All UT System Data, including Data associated with research, must be backed up in accordance with risk management decisions implemented by the Data Owner (See Section 9.)

5.2 All Data Owners with each Entity shall adopt a backup and recovery plan commensurate with the risk and value of the computer system and Data. The backup and recovery plan must incorporate procedures for the following:

- 5.2.1 Recovering Data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, human error, or system operations errors;
- 5.2.2 Assigning operational responsibility for backup of all servers connected to the applicable network;
- 5.2.3 Scheduling Data backups and establishing requirements for off site storage;
- 5.2.4 Securing onsite / offsite storage and media in transit; and
- 5.2.5 Testing backup and recovery procedures.

6. Change Management

All Entities shall adopt change management processes to ensure secure, reliable and stable operations to which all offices that support Information Resources are required to adhere. The change management process must incorporate procedures for:

- 6.1 Formally identifying, classifying, prioritizing and requesting changes;
- 6.2 Identifying and deploying emergency changes;

- 6.3 Assessing potential impacts of changes;
- 6.4 Authorizing changes and exceptions;
- 6.5 Testing changes;
- 6.6 Change implementation and back-out planning; and
- 6.7 Documenting and tracking changes.

7. Computer Virus Prevention

UT System's network infrastructure and other Information Resources must be continuously protected from threats posed by computer viruses, trojans, worms, and other types of hostile computer programs. All UT System owned and personal computers that connect to the UT System network must run all required protection software and adhere to any other protective measures as required by applicable policies and procedures.

8. Classification of Digital Data

8.1 All Entities shall develop Digital Data classification guidelines and a plan for identifying Digital Data maintained in both central and decentralized areas. Owners of Information Resources within the Entity shall classify Digital Data based on Data sensitivity and risk that is Sensitive.

8.2 An Entity may change its classification of Digital Data upon request by the Data Owner with review and approval by the Entity's Executive Officer and/or Office of Legal Affairs or UT System Office of General Counsel.

9. Risk Management

9.1 All Entities shall conduct and document an information security risk assessment annually that identifies Mission Critical Information Resources in the central and all decentralized areas.

9.2 Owners of Mission Critical Information Resources shall perform a security risk assessment on an annual basis. They shall identify, recommend, and document acceptable risk levels for information resources under their authority. Information Resources must be protected based on sensitivity and risk.

9.3 Custodians of Mission Critical Information Resources shall implement approved mitigation strategies and adhere to information security policies and procedures to manage risk levels for information resources under their care.

9.4 The confidentiality and integrity of Sensitive Digital Data must be managed as required by this Policy.

9.5 Digital Data that is not identified as Sensitive must be managed according to applicable standards and policies and, in the case of Research Data, according to federal guidelines for the responsible conduct of Research.

10. Reduction of Use and Collection of Social Security Numbers

UT System recognizes the special risks associated with the collection, use and disclosure of social security numbers. Accordingly, the requirements of this Section 10 apply to social security numbers contained in any medium, including paper records that are collected, maintained, used or disclosed by any Entity except UTIMCO.

10.1 All Entities shall reduce the use and collection of social security numbers.

10.1.1 All Entities shall discontinue the use 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.

10.1.2 If the collection and use of social security numbers is permitted, but not required, by applicable law, the Entity shall use and collect social security numbers only as reasonably necessary for the proper administration or accomplishment of the their respective business, governmental, educational and medical purposes, including, but not limited to:

10.1.2.1 As means of identifying an individual for whom a unique identification number is not known;

10.1.2.2 For internal verification or administrative purposes; and

10.1.2.3 Use for verification or administrative purposes by a third party or agent conducting the Entity's business on behalf of the Entity where the third party or agent has contracted to comply with the safeguards described in Section 11 of this Policy.

10.1.3 Except in those instances in which an Entity is legally required to collect a social security number, an individual shall not be required to disclose 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 Entity'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 Policy. Examples of federal and state laws that require the collection or use of social security numbers are included in Appendices 2 and 3. 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.

10.1.4 An Entity 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.

10.1.5 All Entities 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 Entity.

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

10.1.6.1 Be a component of a system that provides a mechanism for the public identification of individuals;

10.1.6.2 Be permanent and unique within the Entity as applicable and remain the property of, and subject to the rules of, that Entity; and

10.1.6.3 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.

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

10.2 All Entities shall inform individuals when they collect social security numbers

10.2.1 Each time an Entity 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 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.

10.2.1.1 The notice shall use the applicable text from Appendix 4 of this Policy or such other text as may be approved by the Information Security Officer who will consult with the Office of General Counsel with respect to the interpretation of law.

10.2.1.2 It is preferable that the notice be given in writing, but if at times it will be given orally, procedures shall be implemented to assure and document that the notice is properly and consistently given.

10.2.1.3 Existing stocks of forms need not be reprinted with the disclosure notice; the notice may be appended to the form. Future forms and reprints of existing stock shall include the notice printed on the form.

10.2.2 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.

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

10.4 All Entities shall reduce the public display of social security numbers.

10.4.1 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.

10.4.2 The social security number may not be displayed on documents that can be widely seen by the general public (such as time cards, rosters, web pages, and bulletin board postings) unless required by law. This section does not prohibit the inclusion of the social security number on transcripts or on materials for federal or state Data reporting requirements.

10.4.3 If an Entity sends materials containing social security numbers through the mail, it shall take reasonable steps to place the social security number on the document so as not to reveal the number in the envelope window.

10.4.4 The Entity 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 Entity 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).

10.4.5 The Entity shall not print or cause an individual's social security number to be printed on a card or other device required to access a product or service provided by or through the Entity.

- 10.5 All Information Systems acquired or developed must comply with the following:
- 10.5.1 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;
 - 10.5.2 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 Policy;
 - 10.5.3 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
 - 10.5.4 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.

11. Management of Sensitive Digital Data

- 11.1 Each Entity's policies, standards, and/or procedures must describe and require appropriate steps to protect Sensitive Digital Data (e.g., social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law) stored on UT System's computing devices.
- 11.2 All Entities shall control and monitor access to its Sensitive Digital Data based on Data sensitivity and risk (as determined in accordance with Section 9 of this Policy) and by the use of appropriate physical and technical safeguards.
- 11.2.1 All Entities shall limit access to records containing Sensitive Digital Data to those employees who need access to the Data for the performance of the employees' job responsibilities.
 - 11.2.1.1 Employees may not request disclosure of Sensitive Digital Data if it is not necessary and relevant to the purposes of UT System and the particular function for which the employee is responsible.
 - 11.2.2 All Entities shall monitor access to records containing Sensitive Digital Data by the use of appropriate measures as reasonably determined by the Entity.
 - 11.2.3 Employees may not disclose Sensitive Digital Data to unauthorized persons or entities except:
 - As required or permitted by law;
 - With the consent of the individual;
 - Where the third party is the agent or contractor for the Entity and the safeguards described in Section 11.2.4 are in place to prevent unauthorized distribution; or

- As approved by the Office of General Counsel.

11.2.4 If an Entity intends to provide Sensitive Digital Data to a third party acting as an agent of or otherwise on behalf of that Entity (e.g., an application service provider) and if it determines that its provision of Sensitive Digital Data to a third party will result in a significant risk to the confidentiality and integrity of such Data, a written agreement with the third party is required which must specify terms and conditions that protect the confidentiality and integrity of the Sensitive Digital Data as required by this Policy. The written agreement must require the third party to use appropriate administrative, physical, and technical safeguards to protect the confidentiality and integrity of all Sensitive Digital Data obtained and the Entity, as applicable, should monitor compliance with the provisions of the written agreement.

11.3 All Entities shall implement security safeguards to protect its Sensitive Digital Data. Such safeguards shall be appropriate to the sensitivity of the Digital Data to be protected based on risk and, in the case of Research, the research project requirements for that Sensitive Digital Data.

11.3.1 Sensitive Digital Data shall be secured in accordance with each Entity's security plan and with this Policy.

11.3.2 All Entities shall protect the security of records containing Sensitive Digital Data during storage using physical and technical safeguards (such safeguards may include encrypting electronic records, including backups, and locking physical files.)

11.3.3 Unless otherwise required by federal or state law or regulation, Sensitive Digital Data must not be stored on UT System or personal computers or other electronic devices (e.g., laptop, hand-held device, Flash drives, or other Portable Computing Devices) unless:

11.3.3.1 It is secured against unauthorized access in accordance with this Policy;

11.3.3.2 It will not compromise business or Research efforts or privacy interests if lost or destroyed; and

11.3.3.3 The Entity has specific procedures in place that address this subsection.

11.4 All Entities shall discard Electronic media (e.g., disks, tapes, hard drives, etc) containing Sensitive Digital Data as follows:

11.4.1 In a manner that adequately protects the confidentiality of the Sensitive Digital 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

11.4.2 In accordance with the applicable Entity's records retention schedule.

11.5 All Entities shall, based on risk, implement all appropriate technical safeguards necessary to adequately protect the security of Sensitive Digital Data during electronic communications or transmissions.

12. Electronic Communications

All Entities shall require each faculty member, staff, and student to exercise prudence in the use of Electronic Communications and use them in accordance with the Entity's policies, standards, and/or procedures related to Information Resources acceptable use and retention.

13. Incident Management

13.1 Incidents involving computer security will be reported as required by state or federal Law.

13.2 All Entities shall establish and follow Incident Management Procedures to ensure that each incident is reported, documented and resolved in a manner that restores operation quickly while meeting the legal requirements for handling of evidence.

13.3 All Entities shall require employees to report promptly unauthorized or inappropriate disclosure of Sensitive Digital Data, including social security numbers; to their supervisors, Information Security Officer, and/or Entity's compliance hotline.

13.4 Custodians of Mission Critical Information Resources shall implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

13.5 All Entities shall report significant information security incidents, as defined by the [UT System Security Incident Reporting Guidelines](#), to the UT System CISO. Incidents resulting in unauthorized disclosure of University Confidential Data must be reported immediately. Entities shall report incidents to the UT System CISO prior to reporting to non UT System agencies or organizations except as required by state or federal law.

13.6 All Entities shall disclose in accordance with applicable federal and state law, incidents involving computer security that compromises the security, confidentiality, or integrity of Personal Identifying Information it maintains to any resident of Texas and Data Owners whose Personal Identifying Information was, or is reasonably believed to have been, acquired without authorization.

13.6.1 Disclosure shall be made as quickly as possible upon the discovery or receipt of notification of the incident taking into consideration (a) the time necessary to determine the scope of incident and restore the reasonable integrity of operations or (b) any request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be

made as soon as the law enforcement agency determines that it will not compromise the investigation.

13.7 Entities' Incident Management Procedures must incorporate procedures for the following:

13.7.1 Formally identifying, reporting, and classifying incidents;

13.7.2 Responding to incidents;

13.7.3 Assessing potential damage of incidents;

13.7.4 Gathering and preserving physical and electronic evidence;

13.7.5 Assigning responsibility for gathering, maintaining, and reporting detailed information regarding incidents of local and UT System-wide significance; actions taken to remediate; and documentation of a management action plan to prevent a recurrence in accordance with Section 1 of this Policy;

13.7.6 Notifying appropriate System Administration officials, residents of Texas, Data Owners, and consumer reporting agencies as required by applicable state and federal law and UT System policy;

13.7.7 Determining the timing requirements for incident disclosure and notification; and

13.7.8 Determining the appropriate medium to provide notice based on incident significance and number of individuals adversely impacted.

14. Internet Use

14.1 The UT System recognizes that there are risks associated with the posting or consuming of information on the Internet. To mitigate these risks, UT System network Users must adhere to prudent and responsible Internet use practices as outlined in the Entity's policies associated with Information Resources acceptable use.

14.2 All Entities will develop and adhere to policies, standards and/or procedures governing the secure transmission of Confidential University Data via public networks. These policies, standards and/or procedures must incorporate procedures for the following:

14.2.1 Encrypting all Confidential University Data or any specific Data identified as confidential by federal and state law transmitted over the Internet.

15. Information Services (IS) Privacy

Users have no personal expectation of privacy pertaining to electronic files and Data created, sent, received, or stored on computers and other Information Resources owned,

leased, administered, or otherwise under the custody and control of UT System. Files and Data may be accessed as needed for purposes of system administration and maintenance, for resolution of technical problems, for compliance with the Texas Public Information Act, for compliance with federal and state subpoenas, court orders, litigation holds, or other written authorizations, to perform audits, or to otherwise conduct the business of UT System.

16. Network Access

16.1 All network Users are required to acknowledge and abide by all policies relating to Information Resources acceptable use.

16.2 The office or offices charged with maintaining the IT infrastructure at each Entity are required to approve all access methods, installation of all network hardware connected to the local-area network and methods and requirements for attachment of any non UT System owned computer systems or devices to the UT System network to ensure that access to the network does not compromise the operations and reliability of the network, or compromise the integrity or use of information contained within the network.

17. Network Configuration

All Entities must designate responsibility for the Entity's network infrastructure and specify those responsible for configuration and management of the resource to ensure reliability of operations, proper accessibility to resources and protection of Data confidentiality and integrity.

18. Passwords

18.1 In order to preserve the security of Entity Information Resources and Data strong passwords shall be used to control access to Information Resources. All passwords must be constructed, implemented, and maintained according to the requirements of the [UT System Identity Management Federation Member Operating Practices \(MOP\)](#) and applicable policies, standards, and/or procedures governing password management. The Entity's policies, standards and/or procedures must incorporate procedures for the following:

18.1.1 Vetting User identity when issuing or resetting a password;

18.1.2 Establishing password strength;

18.1.3 Changing passwords;

18.1.4 Managing security tokens when applicable; and

18.1.5 Securing unattended computing devices from unauthorized access.

18.2 Users shall not share passwords or similar information or devices used for identification and authorization purposes.

19. Physical Access

19.1 All Information Resources must be physically protected, based on risk, as determined in accordance with Section 9 of this Policy, and associated risk management decisions as part of the overall security program for the UT System.

19.2 All Entities shall adopt Physical Access Safeguards to ensure appropriate granting, controlling, and monitoring of physical access. All offices that own or maintain Information Resources are required to adhere to such Physical Access Safeguards. The Entity's Physical Access Safeguards must incorporate procedures for the following:

19.2.1 Protecting facilities in proportion to the criticality or importance of their function and the confidentiality of any impacted Information Resources affected;

19.2.2 Managing access cards, badges and/or keys;

19.2.3 Changing and/or removing physical access to facilities to reflect changes on User role or employment status; and

19.2.4 Providing access to facilities to Visitors and Vendors.

20. Portable Computing and Remote Access

20.1 To preserve the integrity, availability, and confidentiality of UT System information, Users accessing the Entity's infrastructure remotely must do so in accordance with Section 3 and all policies on Information Resource acceptable use.

20.2 All Entities must develop policies, standards and/or procedures governing remote access and wireless connectivity.

21. Security Monitoring

In accordance with Section 1 of this Policy, all Entities shall have an IT organization that is charged with providing security for all network resources, in both central and decentralized areas, and has the responsibility and Entity-wide authority to monitor network traffic and use of Information Resources to confirm that security practices and controls are adhered to and are effective. Any exceptions to required information security practices must include provisions that ensure compliance with this policy and must be approved and documented by the Entity's Information Security Officer.

22. Security Training

22.1 All Entities shall deliver security awareness General Compliance training in accordance with the following schedule, or more frequently as determined by that Entity:

22.1.1 Training of all Users with access to the Entity's Information Resources shall take place at least yearly; and

22.1.2 To each new, temporary, contract, assigned, or engaged employee or worker within 30 days after the date that such a person is (a) hired by the Entity or (b) otherwise engaged or assigned to perform such work.

22.2 All Entities shall provide appropriate technical training to employees providing information technology help-desk or technical support as determined by that Entity.

23. Server and Network Device Hardening Standards

To protect against malicious attack, all Servers on UT System networks will be security hardened based on risk analysis and must be administered according to policies, standards procedures prescribed by the Entity, as applicable, and must incorporate procedures for the following:

23.1 Managing the testing and installation of security patches; and

23.2 Setting baseline security "hardened" configuration standards for all network device types (examples: routers, laptops, desktops, and PDA's.)

24. Software Licensing

All software installed on UT System owned computers must be used in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious matter subject to disciplinary action and any such use is without the consent of UT System.

25. System Development and Deployment

25.1 All Entities must ensure that the protection of Information Resources (including Data confidentiality, integrity, and accessibility) is considered during the development or purchase of new computer applications or services. The Entity's policies, standards and/or procedures must, at minimum, incorporate procedures for the following:

25.1.1 Providing methods for appropriately restricting privileges of authorized Users to all production systems and applications. User access to applications is granted on a need-to-access basis; and

25.1.2 Maintaining separate production and development environments to ensure the security and reliability of the production system. Exceptions to this must be approved by the Entity's Information Resources Manager.

25.2 The Entity ISO must review the data security requirements and specifications of any new computer applications or services that receive, maintain, and/or share Confidential Data.

25.3 The Entity ISO must approve the security requirements of the purchase of required information technology hardware, software, and systems development services for any new computer applications that receive, maintain, and/or share Confidential Data.

25.4 Information technology contracts 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. Vendors must adhere to all state and federal laws and Regents' Rules and UT System policies pertaining to the protection of Information Resources and privacy of Sensitive Data.

26. Vendor Access

The UT System recognizes that vendors serve an important function in the support of services, hardware and software and, in some cases, the operation of computer networks, servers, and/or applications.

26.1 Vendors contracts must require that vendors comply with all applicable UT System rules associated with this policy, practice standards and agreements, and address all federal and state laws to which UT System must adhere to ensure that UT System remains in compliance with such law.

26.2 All Entities shall control Vendor access to its Sensitive Data based on data sensitivity and risk (as determined in accordance with Section 9 of this Policy) and by the use of appropriate measures. Such measures must incorporate the following:

26.2.1 Vendor shall represent, warrant and certify it will:

26.2.1.1 Hold all Sensitive Data in the strictest confidence;

26.2.1.2 Not release any Sensitive Data concerning an Entity student unless Vendor obtains Entity's prior written approval and performs such a release in full compliance with all applicable privacy laws, including FERPA;

26.2.1.3 Not otherwise use or disclose Sensitive Data except as required or permitted by law;

26.2.1.4 Safeguard Sensitive 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);

26.2.1.5 Continually monitor its operations and take any action necessary to assure the Sensitive Data is safeguarded in accordance with the terms of this Policy; and

26.2.1.6 Comply with the Vendor Access Requirements that are set forth in this section.

26.2.2 To the extent that the Sensitive Data includes Protected Health Information (“PHI”) as defined in 45 CFR § 164.501, if required by an Entity, Vendor shall execute a HIPAA Business Associate agreement in the form required by UT System.

26.2.3 Entities shall require the following from the Vendor:

26.2.3.1 If an unauthorized use or disclosure of any Sensitive Data occurs, the Vendor must provide:

26.2.3.1.1 Written notice within one (1) business day after Vendor’s discovery of such use or disclosure and

26.2.3.1.2 All information UT System requests concerning such unauthorized use or disclosure.

26.2.3.2 Within 30 days after the termination or expiration of a Purchase Order, Contract or Agreement for any reason, Vendor shall either:

26.2.3.2.1 Return or destroy, as applicable, all Sensitive Data provided to the Vendor by Entity to Vendor, including all Sensitive Data provided to Vendor’s employees, subcontractors, agents, or other affiliated persons or entities; or

26.2.3.2.2 In the event that returning or destroying the Sensitive Data is not feasible, provide notification of the conditions that make return or destruction not feasible, in which case, the Vendor must continue to protect all Sensitive Data that it retains and agree to limit further uses and disclosures of such Data to those purposes that make the return or destruction not feasible as Vendor maintains such Data.

27. Right to Monitor

Entities have the authority and responsibility to monitor Information Resources in accordance with TAC 202.75 (7) (P):

27.1 To ensure compliance with this policy and state laws and regulations related to the use and security of Information Resources; and

27.2 To ensure that information resources security controls are in place, are effective, and are not being bypassed.

28. Disciplinary Actions

Violation of this policy may result in disciplinary action for faculty, staff and students in accordance to each Entity’s rules and policies. For contractors and consultants this may include termination of the work engagement. For interns and volunteers, this may include dismissal. Any student who violates this policy will be referred to student judicial services at the student’s home campus. Additionally, all individuals are subject to possible civil and criminal prosecution.

SPECIAL REQUIREMENTS FOR INITIAL IMPLEMENTATION OF POLICY

This Policy is based on public policy and privacy issues and not on convenience or past practices. Nevertheless, the UT System recognizes the financial burdens and the potentially disruptive nature of securing, reprogramming and immediate conversions of business, research, and information systems.

Nothing in this Policy is intended to prohibit or restrict the collection, use, and maintenance of Sensitive Data as required or permitted by applicable law, to create unjustified obstacles to the conduct the business of the UT System and the provision of services to its many constituencies or negatively affect UT System's commitment to engage in high-quality, innovative Research that entails the discovery, retention, dissemination, and application of knowledge in compliance with UT System policy and state and federal laws and regulations.

FORMS AND TOOLS/ONLINE PROCESSES

Template for an Acceptable Use Policy is available at the following address:
http://www.utsystem.edu/ciso/documents/SystemWideAcceptableUseTemplate_1208.doc

APPENDIX

[Appendix 1](#): Chronological Implementation Plan for Protection of the Confidentiality of Social Security Numbers

[Appendix 2](#): Examples of Federal Laws Requiring the Use or Collection of Social Security Numbers

[Appendix 3](#): Examples of State Laws Requiring the Use or Collection of Social Security Numbers

[Appendix 4](#): Pre-approved Text for Notice Required by the Federal Privacy Act of 1974

[Information Security Practice Bulletin #1: Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices](#)

[Information Security Practice Bulletin #2: Baseline Standard for Information Security Programs](#)

Bulletin #2 Corresponding Documents

- [UT System Information Security Program Elements](#)
- [UT System Information Security Program Metrics Reported to UT System](#)
- [Institutional Information Security Program Quarterly Status Report Template](#)

Keywords: acceptable use, security, information technology, internet, email, social security numbers, confidentiality, data, research, computers, computer, technology, internet, IT, information technology (IT), social security number, web, password, passwords, compliance, internet usage
