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

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

Sec. 4 Compliance with State Law. Information that is collected pursuant or related to the U. T. System Information Security Program is subject to Section 552.139 of the Texas Government Code and is therefore confidential by law. Accordingly, an Institution may not withhold information or fail to include

information required by this Policy and/or Security Standards to be provided to or included in the U. T. System Information Security Program or for administration of program oversight.

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

UTS165 Standard 1. Information Resources Security Responsibilities and Accountability
UTS165 Standard 2. Acceptable Use of Information Resources
UTS165 Standard 3. Information Security Programs
UTS165 Standard 4. Access Management
UTS165 Standard 5. Administrative/Special Access Accounts
UTS165 Standard 6. Backup and Disaster Recovery
UTS165 Standard 7. Change Management
UTS165 Standard 8. Malware Prevention
UTS165 Standard 9. Data Classification
UTS165 Standard 10. Risk Management
UTS165 Standard 11. Safeguarding Data
UTS165 Standard 12. Security Incident Management
UTS165 Standard 13. Use and Protection of Social Security Numbers
UTS165 Standard 14. Information Services (IS) Privacy
UTS165 Standard 15. Passwords
UTS165 Standard 16. Data Center Security
UTS165 Standard 17. Security Monitoring
UTS165 Standard 18. Security Training
UTS165 Standard 19. Server and Device Configuration and Management
UTS165 Standard 20. Software Licensing
UTS165 Standard 21. System Development and Deployment
UTS165 Standard 22. Vendor Controls and Compliance
UTS165 Standard 23. Security Control Exceptions
UTS165 Standard 24. Disciplinary Actions

Sec. 6 Information Resources Acceptable Use.

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

6.2 Reasonableness of Personal Use. Users are responsible for exercising good judgment regarding the reasonableness of personal use in accordance with all Policies associated with Information Resources acceptable use.

6.3 Incidental Personal Use. As a convenience to the U. T. System User community, limited incidental personal use of Information Resources is permitted.

6.4 Direct Cost or Risk. Incidental use of Information Resources must not result in direct cost to the U. T. System or expose U. T. System to unnecessary risks.

Sec. 7 Account Management. The U. T. System recognizes that proper management and use of computer accounts are basic requirements for protecting U. T. 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 U. T. 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:

7.1 creating uniquely identifiable accounts for all Users. This includes accounts created for use by outside Vendors (see Section 31);

7.2 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

7.3 expiring or disabling passwords at least annually or more often if warranted by risk.

Sec. 8 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:

8.1 acceptable use of administrative/special access accounts and intended administrative purposes;

8.2 authorizing use of administrative/special access accounts;

8.3 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

8.4 escrowing login passwords for each secured system for access during emergencies. Individual User login passwords shall not be escrowed.

Sec. 9 Backup Recovery of Network Servers and Data.

9.1 Backup 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 (see Section 14).

9.2 Backup and Recovery Plan. 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:

(a) 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;

(b) assigning operational responsibility for backup of all servers connected to the applicable network;

(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.

Sec. 10 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:

10.1 formally identifying, classifying, prioritizing and requesting changes;

10.2 identifying and deploying emergency changes;

10.3 assessing potential impacts of changes;

10.4 authorizing changes and exceptions;

10.5 testing changes;

10.6 change implementation and back-out planning; and

10.7 documenting and tracking changes.

Sec. 11 Computer Virus Prevention. U. T. 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 U. T. System owned and personal computers that connect to the U. T. System network must run all required protection software and adhere to any other protective measures as required by applicable policies and procedures.

Sec. 12 Classification of Digital Data.

12.1 Guidelines. 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. Sensitive Digital Data is defined in Section 14.4 of this Policy.

12.2 Classification Changes. 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 U. T. System Office of General Counsel.

Sec. 13 Risk Management.

13.1 Annual Assessment. 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.

13.2 Owners. 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.

13.3 Custodians. 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.

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

- federal agencies (e.g., Food and Drug Administration);
- State agencies (e.g., data defined as High-Risk Information Resources by 1 Texas Administrative Code 202.72);
- employee benefit providers;
- Office of General Counsel or Entity Office of Legal Affairs (i.e., data subject to or involved in litigation or confidentiality agreements);
- intellectual property and/or technology transfer requirements; or
- federal regulations (e.g., FERPA, HIPAA, Gramm-Leach-Bliley, Biodefense, Homeland Security, Department of Defense, etc.)

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

13.5 Nonsensitive Digital Data. 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.

Sec. 14 Reduction of Use and Collection of Social Security Numbers. U. T. System recognizes the special risks associated with the collection, use, and disclosure of social security numbers. Accordingly, the requirements of this section apply to social security numbers contained in any medium, including paper records that are collected, maintained, used or disclosed by any Entity except UTIMCO.

14.1 Reduction of Use and Collection. All Entities shall reduce the use and collection of social security numbers.

(a) 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.

(b) 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 respective business, governmental, educational, and medical purposes, including, but not limited to:

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

ii. for internal verification or administrative purposes; and

iii. 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 16 of this Policy.

(c) 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 ISO who will consult with the Office of General Counsel with respect to the interpretation of law.

(d) 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.

(e) 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.

(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 Entity as applicable and remain the property of, and subject to the rules of, that Entity; 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.

14.2 Notification. All Entities shall inform individuals when they collect social security numbers.

(a) 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.

i. The notice shall use the applicable text from Appendix 4 of this Policy or such other text as may be approved by the ISO in consultation with the Office of General Counsel.

ii. 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.

iii. 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.

(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 *Texas Government Code*, the individual is entitled to receive and review the information; and under Section 559.004 of the *Texas Government Code*, the individual is entitled to have the incorrect information about the individual corrected.

14.3 Prohibition of Personal Use. Employees may not seek out or use social security numbers relating to others for their own interest or advantage.

14.4 Public Display. All Entities shall reduce the public display of social security numbers.

(a) 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.

(b) 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.

(c) 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.

(d) 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).

(e) 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.

14.5 Compliance. 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 Policy;

(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.

Sec. 15 Management of Sensitive Digital Data.

15.1 Protection. 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 U. T. System's computing devices.

15.2 Access. All Entities shall control and monitor access to their Sensitive Digital Data based on Data sensitivity and risk (as determined in accordance with Section 14 of this Policy) and by the use of appropriate physical and technical safeguards.

(a) 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.

Employees may not request disclosure of Sensitive Digital Data if it is not necessary and relevant to the purposes of U. T. System and the particular function for which the employee is responsible.

(b) All Entities shall monitor access to records containing Sensitive Digital Data by the use of appropriate measures as reasonably determined by the Entity.

(c) Employees may not disclose Sensitive Digital Data to unauthorized persons or entities except:

i. as required or permitted by law;

ii. with the consent of the individual;

iii. where the third party is the agent or contractor for the Entity and the safeguards described in Section 16.2(d) are in place to prevent unauthorized distribution; or

iv. as approved by the Office of General Counsel.

(d) 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 that 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.

15.3 Security Safeguards. All Entities shall implement security safeguards to protect their 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.

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

(b) 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).

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

i. it is secured against unauthorized access in accordance with this Policy;

ii. it will not compromise business or Research efforts or privacy interests if lost or destroyed; and

iii. the Entity has specific procedures in place that address this section.

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

(a) 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

(b) in accordance with the applicable Entity's records retention schedule.

15.5 Electronic Communications or Transmissions. 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.

Sec. 16 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.

Sec. 17 Incident Management.

17.1 Reporting Requirements. Incidents involving computer security will be reported as required by State or federal law.

17.2 Incident Management Procedures. 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.

17.3 Employee Reporting. All Entities shall require employees to report promptly unauthorized or inappropriate disclosure of Sensitive Digital Data, including social security numbers, to their supervisors, ISO, and/or the Entity's compliance hotline.

17.4 Monitoring Techniques and Procedures. Custodians of Mission Critical Information Resources shall implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

17.5 Reporting Guidelines. All Entities shall report significant information security incidents, as defined by the U. T. System Security Incident Reporting Guidelines, to the U. T. System CISO. Incidents resulting in unauthorized disclosure of Confidential University Data must be reported immediately. Entities shall report 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.

17.6 Disclosure. All Entities shall disclose in accordance with applicable federal and State law, incidents involving computer security that compromise the security, confidentiality, or integrity of Personal Identifying Information they maintain to any resident of Texas and Data Owners whose Personal Identifying Information was, or is reasonably believed to have been, acquired without authorization.

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.

17.7 Incident Management Procedures Content. Entities' Incident Management Procedures must incorporate procedures for the following:

(a) formally identifying, reporting, and classifying incidents;

(b) responding to incidents;

(c) assessing potential damage of incidents;

(d) gathering and preserving physical and electronic evidence;

(e) assigning responsibility for gathering, maintaining, and reporting detailed information regarding incidents of local and U. T. Systemwide significance; actions taken to remediate; and documentation of a management action plan to prevent a recurrence in accordance with Section 6 of this Policy;

(f) notifying appropriate System Administration officials, residents of Texas, Data Owners, and consumer reporting agencies as required by applicable State and federal law and U. T. System policy;

(g) determining the timing requirements for incident disclosure and notification; and

(h) determining the appropriate medium to provide notice based on incident significance and number of individuals adversely impacted.

Sec. 18 Internet Use.

18.1 Risks. The U. T. System recognizes that there are risks associated with the posting or consuming of information on the Internet. To mitigate these risks, U. T. 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.

18.2 Policies, Standards, and Procedures. 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 encrypting all Confidential University Data or any specific Data identified as confidential by federal and State law transmitted over the Internet.

Sec. 19 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 U. T. 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 U. T. System.

Sec. 20 Network Access.

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

20.2 Approvals. 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-U. T. System owned computer systems or devices to the U. T. 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.

Sec. 21 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.

Sec. 22 Passwords.

22.1 Procedures. 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 U. T. System Identity Management Federation and applicable policies, standards, and/or procedures governing password management. The Entity's policies, standards, and/or procedures must incorporate procedures for the following:

(a) vetting User identity when issuing or resetting a password;

(b) establishing password strength;

(c) changing passwords;

(d) managing security tokens when applicable; and

(e) securing unattended computing devices from unauthorized access.

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

Sec. 23 Physical Access.

23.1 Protection. All Information Resources must be physically protected, based on risk, as determined in accordance with Section 14 of this Policy, and associated risk management decisions as part of the overall security program for the U. T. System.

23.2 Safeguards. 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:

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

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

(c) changing and/or removing physical access to facilities to reflect changes on User role or employment status; and

(d) providing access to facilities to visitors and Vendors.

Sec. 24 Portable Computing and Remote Access.

24.1 User Responsibilities. To preserve the integrity, availability, and confidentiality of U. T. System information, Users accessing the Entity's infrastructure remotely must do so in accordance with Section 8 and all policies on Information Resource acceptable use.

24.2 Policies, Standards, and Procedures. All Entities must develop policies, standards, and/or procedures governing remote access and wireless connectivity.

Sec. 25 Security Monitoring. In accordance with Section 6 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 ISO.

Sec. 26 Security Training.

26.1 User Training. All Entities shall deliver security awareness general compliance training in accordance with the following schedule, or more frequently as determined by that Entity:

(a) training of all Users with access to the Entity's Information Resources shall take place at least yearly; and

(b) training of each new, temporary, contract, assigned, or engaged employee or worker shall take place 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.

26.2 Technical Support Training. All Entities shall provide appropriate technical training to employees providing IT help desk or technical support as determined by that Entity.

Sec. 27 Server and Network Device Hardening Standards. To protect against malicious attack, all Servers on U. T. System networks will be security hardened based on risk analysis and must be administered according to policies and standards procedures prescribed by the Entity, as applicable, and must incorporate procedures for the following:

27.1 managing the testing and installation of security patches; and

27.2 setting baseline security "hardened" configuration standards for all network device types (examples: routers, laptops, desktops, and personal digital assistants).

Sec. 28 Software Licensing. All software installed on U. T. 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 U. T. System.

Sec. 29 System Development and Deployment.

29.1 Procedures. 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 a minimum, incorporate procedures for the following:

(a) 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

(b) 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 IRM.

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

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

29.4 Contracts. IT 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 Regulations* and U. T. System policies pertaining to the protection of Information Resources and privacy of Sensitive Data.

Sec. 30 Vendor Access. The U. T. 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.

30.1 Contracts. Vendor contracts must require that Vendors comply with all applicable U. T. System rules associated with this policy, practice standards, and agreements, and address all federal and State laws to which U. T. System must adhere to ensure that U. T. System remains in compliance with such law.

30.2 Access Control Measures. All Entities shall control Vendor access to their Sensitive Data based on data sensitivity and risk (as determined in accordance with Section 14 of this Policy) and by the use of appropriate measures. Such measures must incorporate the following:

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

i. hold all Sensitive Data in the strictest confidence;

ii. 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 the Family Educational Rights and Privacy Act (FERPA);

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

iv. 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);

v. 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

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

(b) To the extent that the Sensitive Data includes PHI as defined in 45 C.F.R. § 164.501, if required by an Entity, Vendor shall execute a Health Insurance Portability and Accountability Act (HIPAA) business associate agreement in the form required by U. T. System.

(c) Entities shall require the following from the Vendor:

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

A. written notice within one business day after Vendor's discovery of such use or disclosure; and

B. all information U. T. System requests concerning such unauthorized use or disclosure.

ii. Within 30 days after the termination or expiration of a purchase order, contract, or agreement for any reason, Vendor shall either:

A. return or destroy, as applicable, all Sensitive Data provided to the Vendor by the Entity, including all Sensitive Data provided to Vendor's employees, subcontractors, agents, or other affiliated persons or entities; or

B. 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.

Sec. 31 Right to Monitor. Entities have the authority and responsibility to monitor Information Resources in accordance with *Texas Administrative Code* 202.75(7)(P):

31.1 to ensure compliance with this policy and State laws and regulations related to the use and security of Information Resources; and

31.2 to ensure that Information Resources security controls are in place, are effective, and are not being bypassed.

Sec. 32 Disciplinary Actions. Violation of this policy may result in disciplinary action for faculty, staff, and students in accordance with 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.

Sec. 33 Special Requirements for Initial Implementation of Policy.

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 conduct the business of the U. T. System and the provision of services to its many constituencies; or to negatively affect U. T. System's commitment to engage in high-quality, innovative Research that entails the discovery, retention, dissemination, and application of knowledge in compliance with Regents' *Rules and Regulations*, U. T. System Policies, and State and federal laws and regulations.

3. 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.

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

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 U. T. 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, maintained, or made available in electronic media.

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 websites, 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 assistants (PDAs), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources 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.

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 that, 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 capable of receiving, transmitting, and/or storing electronic data and 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.

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, pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs and similar storage devices.

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

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. This individual 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 U. T. System’s investment assets.

U. T. 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 U. T. System who exchanges goods or services for money or other consideration.

4. Relevant Federal and State Statutes

Title 1 *Texas Administrative Code* 202.2 Information Security Standards Institutions of Higher Education

Texas Education Code § 65.31Administration of The University of Texas System General Powers and Duties

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 Confidentiality of Social Security Numbers

Texas Government Code § 559.003 Right to Notice About Certain Information and Practices

5. Relevant System Policies, Procedures, and Forms

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

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: Preapproved 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

- U. T. System Information Security Program Elements
- U. T. System Information Security Program Metrics Reported to U. T. System
- Institutional Information Security Program Quarterly Status Report Template

6. System Administration Office(s) Responsible for Policy

Office of Technology and Information Services

7. Dates Approved or Amended

April 12, 2007
June 15, 2010
August 15, 2012