

Information Resources Use and Security Policy

1. Overview	2
2. Policy Statement	2
3. Rationale	3
4. Audience	3
5. Procedures	3
5.1. Information Resources Security Responsibility and Accountability	3
5.2. Acceptable Use	6
5.3. Account Management	7
5.4. Administrative/Special Access	7
5.5. Backup Recovery of Systems and Data	8
5.6. Change Management.....	9
5.7. Computer Virus Protection	10
5.8. Classification of Sensitive (Category-I) Digital Data	10
5.9. Risk Management	11
5.10. Reduction of Use and Collection of Social Security Numbers.....	11
5.11. Management of Sensitive Digital Data	15
5.12. Electronic Mail (E-mail)	17
5.13. Incident Management.....	17
5.14. Internet Use	19
5.15. Information Services Privacy.....	19
5.16. Network Access.....	20
5.17. Network Configuration	20
5.18. Passwords	21
5.19. Physical Access.....	22
5.20. Portable Computing and Remote Access.....	24
5.21. Security Monitoring	25
5.22. Security Training	25

Information Resources Use and Security Policy

Document Version: Approved

5.23.	System Hardening	25
5.24.	Software Licensing	26
5.25.	Secure Development and Administration.....	26
5.26.	Vendor Access.....	27
5.27.	Right to Monitor.....	28
5.28.	Disciplinary Actions	28
6.	Implementation	29
7.	Appendix	29
8.	Definitions.....	29
9.	Revision History	30
10.	Approvals	36

1. Overview

The Information Resources Use and Security Policy provides The University of Texas at Austin with guidance and defines responsibilities and procedures relating to the operational implementation of the [UT System Information Resources Use and Security Policy \(UTS 165\)](#). For ease of reference both documents share the same organizational structure and a common table of contents.

Technical terms referred to in this document are defined in the [ISO Technical and Security Glossary](#).

2. Policy Statement

It is the policy of the university to:

- Protect Information Resources based on risk against accidental or unauthorized disclosure, modification, or destruction and assure the confidentiality, integrity, and availability of university data;
- Appropriately reduce the collection, use, or disclosure of social security numbers contained in any medium, including paper records;
- Apply appropriate physical and technical safeguards without creating unjustified obstacles to the conduct of the business and research of the university and the provision of services to its many constituencies.
- Comply with applicable state and federal laws and UT System rules governing information resources.

3. 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 agencies of State government are strategic and vital assets belonging to the people of Texas. Assets of the university must be available and protected commensurate with their value and must be administered in conformance with federal and state law and UT System [Regents' Rules](#). This Policy provides requirements and guidelines to establish accountability and prudent and acceptable practices regarding the use and safeguarding of the university's 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 the university's information resources.

This policy serves as the foundation for the university's information security program, and provides the Information Security Office the authority to implement policies, practice standards, and/or procedures necessary to implement a successful information security program in compliance with this policy.

4. Audience

The Information Resources Use and Security Policy provides guidance for all individuals that have, or may require, access to Information Resources at The University of Texas at Austin, and those with responsibility for maintaining its Information Resources. All university colleges, schools, and business units are encouraged to develop policies and procedures specific to their unique environments as needed, so long as they do not conflict with or weaken the policy statements instituted by the university or UT System or any federal or state laws.

5. Procedures

5.1. Information Resources Security Responsibility and Accountability

5.1.1. The university must designate responsibility for the information security function by documenting key roles and responsibilities.

5.1.2. The Chancellor of UT System shall be responsible for the following:

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

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

5.1.3. The President of the university shall be responsible for the following:

Information Resources Use and Security Policy

Document Version: Approved

- 5.1.3.1. Compliance with this Policy;
 - 5.1.3.2. Budgeting sufficient resources to fund ongoing and continuous information security remediation, implementation, and compliance activities that reduce compliance risk to an acceptably low level;
 - 5.1.3.3. Approving the university's Information Security Program, or designate someone to provide approval; and
 - 5.1.3.4. Ensuring that appropriate corrective and disciplinary action is taken in the event of non-compliance.
- 5.1.4. 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:
- 5.1.4.1. Providing leadership, strategic direction, and coordination for the UT System-wide information security initiative including issuing security practice bulletins relating to standards and best practices;
 - 5.1.4.2. Establishing the UT System CISO Council and hold meetings at least quarterly;
 - 5.1.4.3. Developing and providing oversight for a UT System-wide Information Security Compliance Program. This program shall include UT System-wide and institutional action plans, training plans, and monitoring plans;
 - 5.1.4.4. Providing guidance on the institutional Information Security Program including organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum standards;
 - 5.1.4.5. Defining the risk management process to be used for all information security risk management activities;
 - 5.1.4.6. Exploring and recommending the acquisition of tools and resources that can be utilized UT System-wide and how expertise can be shared among institutions;
 - 5.1.4.7. Establishing reporting guidance, metrics, and timelines and monitoring effectiveness of security strategies at each institution; and
 - 5.1.4.8. Apprising the Chancellor and Board of Regents quarterly on the status and effectiveness of the information security compliance programs and activities at each institution.
- 5.1.5. The university's Chief Information Officer (CIO), who is charged with oversight of information technology for the university shall serve in the functional role of

[Information Resources Manager](#) (IRM) as defined by the state and will have authority for the entire university.

- 5.1.6. The President shall designate an individual other than the Information Resources Manager (IRM) to serve as the university's [Chief Information Security Officer](#) (CISO) who shall serve in the capacity as required by state law and with authority for all of the university. The responsibilities of the CISO shall include the following:
 - 5.1.6.1. Assuring information security for all centrally maintained and all distributed systems and computer equipment;
 - 5.1.6.2. Developing an institutional Information Security Compliance Program. This program shall include institutional action plans, training plans, and monitoring plans;
 - 5.1.6.3. Conducting and documenting an information security assessment annually in accordance with [1 TAC 202.72](#) that identifies Mission Critical Information Resources in the central and decentralized areas;
 - 5.1.6.4. Ensuring an annual information security risk assessment is performed (using the process defined above) by each Owner of Mission Critical Information Resources;
 - 5.1.6.5. Requiring each Owner of Mission Critical Information Resources to designate an Information Security Administrator (ISA);
 - 5.1.6.6. Establishing an Institutional Information Security Working Group composed of ISAs and hold meetings at least quarterly;
 - 5.1.6.7. Documenting and maintaining an up-to-date Institutional Information Security Program. The program shall identify specific mitigation strategies to be used by each Owner of Mission Critical Information Resources to manage identified risk;
 - 5.1.6.8. Establishing reporting guidance, metrics, and timelines and monitoring effectiveness of security strategies in both central and decentralized operations;
 - 5.1.6.9. Communicating instances of non-compliance to appropriate administrative officers for corrective, restorative and/or disciplinary action; and
 - 5.1.6.10. Reporting 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. The report is to include a certification that best efforts have been made to ensure appropriate strategies are being applied consistently over time, and that all security incidents have been reported.

Information Resources Use and Security Policy

Document Version: Approved

- 5.1.7. Owners of Mission Critical Information Resources at the university shall designate an individual to serve as an Information Security Administrator (ISA) to implement information security policies and procedures and to report incidents to the CISO. The responsibilities of the ISA shall include the following:
 - 5.1.7.1. Implementing and complying with all university information technology policies and procedures relating to assigned systems;
 - 5.1.7.2. Reporting general computing and security incidents to the CISO;
 - 5.1.7.3. Assisting, as a member of the ISA Working Group, the CISO in developing, implementing, and monitoring the Information Security Program.
 - 5.1.7.4. Establishing reporting guidance, metrics, and timelines for CISO to monitor effectiveness of security strategies in both the centralized and decentralized operations; and
 - 5.1.7.5. Reporting at least annually to the CISO about the status and effectiveness of information resources security controls.
- 5.1.8. Department Heads and Principal Investigators (PI) at the university 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.
- 5.1.9. The university's Offices of Institutional Compliance and Internal Audit shall provide high-level monitoring of the Information Security Compliance Program through inspections and verifications of reported information and periodic audits respectively.
- 5.1.10. All Users must comply with this policy. Users who fail to comply are subject to disciplinary action in accordance with [Section 28](#).

5.2. Acceptable Use

- 5.2.1. All individuals accessing the university's Information Resources must formally acknowledge and abide by the [Acceptable Use Policy](#). Formal acknowledgement of the Acceptable Use Policy by all individuals accessing the university's Information Resources serves as a compliance and enforcement tool.
- 5.2.2. Users are responsible for exercising good judgment regarding the reasonableness of personal use in accordance with all policies associated with the acceptable use of Information Resources and the [Minimum Security Standards for Data Stewardship](#).
- 5.2.3. As a convenience to the university's User community, limited incidental personal use of Information Resources is permitted.

- 5.2.4. Incidental use of Information Resources must not result in any burden or direct cost to the university or expose it to unnecessary risks.

5.3. Account Management

Proper management and use of computer accounts are basic requirements for protecting the university's Information Resources. All offices that create access accounts for applications, networks, or systems are required to manage the accounts in accordance with the university's access management processes. Access to an Information Resource may not be granted by another User without the permission of the Owner or the Owner's delegated custodian of that Information Resource. All accounts are to be created and managed using the following required account management practices:

- 5.3.1. All accounts that access non-public university Information Resources must follow an account creation process. This process shall document who is associated with the account, the purpose for which the account was created, and who approved the creation of the account. All accounts wishing to access the university's non-public Information Resources must have the approval of the Owner of those resources. These measures also apply to account created by/for use of outside vendors or contractors (see [Section 26](#)).
- 5.3.2. Each account having special privileges must adhere to the university's password requirements (see [Section 18](#)).
- 5.3.3. All accounts must be able to be associated with an identifiable individual or group of individuals that are authorized to use that account (for example, the UT-EID).
- 5.3.4. Accounts of individuals on extended leave (more than 120 days) or accounts that have not been accessed more than 120 days must be disabled.
- 5.3.5. Accounts of individuals who have had their status, roles, or affiliations with university change must be updated to reflect their current status.
- 5.3.6. Accounts must be reviewed at least annually to ensure their current state is correct.
- 5.3.7. Password aging and expiration dates must be enabled, where supported by the underlying accounting mechanism, on all accounts created for outside vendors, external contractors, or those with contractually limited access to the university's information resources.

5.4. Administrative/Special Access

Users must be made aware of the privileges granted to their accounts, especially those that impact access to information resources or that allow them to circumvent controls in order to administer the information resource. Abuse of such privileges will not be tolerated. Anyone using accounts with elevated access privileges of this type must adhere to the following access requirements.

Information Resources Use and Security Policy

Document Version: Approved

- 5.4.1. Individuals who use accounts with special privileges (for example, System Administrators) must use these accounts only for their intended administrative purposes.
- 5.4.2. Individuals who use accounts with special privileges may perform investigations relating to the potential misuse of information resources by an individual user only under the direction of the Information Security Office.
- 5.4.3. All colleges, schools, and units (CSUs) of the university must submit a list of administrative contacts to the Information Technology Services (ITS) Networking group, using ITS provided tools (for example, UTnet management tools) for all systems connected to the university network.
- 5.4.4. All individuals whose accounts have special privileges must complete a [Background Check for Staff/Faculty](#). Additionally, all individuals assigned special privileges should acknowledge their responsibilities by signing a form such as a [Position of Special Trust form](#).
- 5.4.5. The password for a shared administrator/special access account must change when any individual knowing the password leaves the department or university or changes role; or upon a change in the vendor personnel assigned to university contracts having password access.
- 5.4.6. For all systems serving out information resources there must be a password escrow procedure in place to enable someone other than the administrator to gain access to the system in an emergency situation.
- 5.4.7. When special privileges are needed for auditing, software development, software installation, or other defined needs, they:
 - 5.4.7.1. Must be authorized by the appropriate department head or owner;
 - 5.4.7.2. Must be created with an expiration date when supported; and
 - 5.4.7.3. Must be removed and disabled when work is complete.

5.5. Backup Recovery of Systems and Data

Backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, human error, or systems operations errors. The university requires the following backup practices, as warranted by the [Data Classification Standard](#) and commensurate with the risk and value of the system and data:

- 5.5.1. All university data, including data associated with research, must be backed up in accordance with risk management decisions implemented by the Data Owner (see [Section 9](#)). The university's Office of Internal Audit periodically reviews backup plans.
- 5.5.2. Each college, school, or unit responsible for a system(s) maintains a recovery plan that is reviewed periodically by the university's Office of Internal Audit. The recovery plan includes the following:
 - 5.5.2.1. Procedures for recovering data and applications in the case an unexpected event occurs such as a natural disaster, power or system disk failure, espionage, data entry error, human error, or other systems operation errors;
 - 5.5.2.2. Assignments of operational responsibility for backup of all systems connected to the respective network;
 - 5.5.2.3. Requirements for off-site storage needs;
 - 5.5.2.4. Physical and network access controls for on-site and off-site storage;
 - 5.5.2.5. Processes to ensure backups are viable and can be recovered (for example, routine testing of backup and recovery procedures.)

5.6. Change Management

The university's Information Resources infrastructure is constantly changing and evolving to support the mission of the university. Computer networks, systems, and applications require planned outages for upgrades, maintenance, and fine-tuning. The [Change Management Guidelines](#) provide expanded detail for the following change management procedures that are required, as warranted by the [Data Classification Standard](#) and commensurate with the risk and value of the system and/or data:

- 5.6.1. All changes to environmental controls affecting computing facility machine rooms (for example, air-conditioning, water, heat, plumbing, electricity, and alarms) must be logged and reported to the appropriate college, school, or unit managing the systems in that facility.
- 5.6.2. Colleges, schools, or units responsible for information resources will ensure that the change management procedures and processes they have approved are being performed.
- 5.6.3. Colleges, schools, or units may object to a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out contingencies, inopportune timing in terms of impact on service to users or in relation to key business process such as year-end accounting, or lack of resources to address potential problems that may be caused by the change. The responsible party will review all objections.

- 5.6.4. Whenever possible, customers will be notified of changes following the steps contained in the change management procedures.
- 5.6.5. A responsible college, school, or unit, consistent with change management procedures, maintains a [change management log](#) for all significant changes including emergency changes. Change management log entries must contain at least the following information:
 - 5.6.5.1. Date of submission and date of change;
 - 5.6.5.2. Owner and custodian contact information; and
 - 5.6.5.3. The nature of the change.

5.7. Computer Virus Protection

A variety of technologies and practices are required to protect the university's network infrastructure and other information resources from threats posed by computer viruses, worms, and other types of malicious code.

- 5.7.1. All systems connecting to the university network, whether owned by the university or not, must install and enable current virus protection software. Exceptions should be acknowledged by completing a [Security Exception Report](#).
 - 5.7.1.1. University e-mail servers must utilize properly maintained e-mail virus protection software and/or utilize the security services provided by the campus e-mail gateway service; and
 - 5.7.1.2. Any system identified as a security risk due to a lack of virus protection may be disconnected from the network or the respective network account may be disabled until adequate protection is in place.
- 5.7.2. Every known instance of a computer virus infection constitutes a security incident and must be reported to the [Information Security Office](#) in accordance with [Section 13](#) of this Policy. When required, the Information Security Office will initiate Incident Management Procedures and organize a [Computer Incident Response Team \(CIRT\)](#).

5.8. Classification of Sensitive (Category-I) Digital Data

- 5.8.1. All data owners, data stewards, or designated custodians, shall be responsible for classifying Digital Data stored, processed, or transmitted by systems under their purview based on data sensitivity and risk so that the appropriate security controls can be applied.
- 5.8.2. The [Data Classification Standard](#) shall be used to identify Digital Data that is Sensitive.

- 5.8.3. A data classification of Category-I shall be based on compliance with applicable Federal or State law, a contract, or on the demonstrated need to (a) document the integrity of that Digital Data (that is, 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:
- 5.8.3.1. Federal or State agencies (for example, Food and Drug Administration);
 - 5.8.3.2. Employee Benefits Providers;
 - 5.8.3.3. Intellectual Property and/or Technology Transfer requirements;
 - 5.8.3.4. UT System Office of General Counsel or university Office of Legal Affairs (in the case of data subject to or involved in litigation or confidentiality agreements); or
 - 5.8.3.5. Federal regulations (for example, FERPA, HIPAA, Gramm-Leach-Bliley, Biodefense, Homeland Security, DoD, etc.)
- 5.8.4. Category-I Digital Data must include all High-Risk Information Resources as defined by 1 TAC 202.72.
- 5.8.5. Certain Digital Data not defined as a High-Risk Information Resource by 1 TAC 202.72 can be classified as Category-I Digital Data if warranted by the college, school, or unit's demonstrated need. With suitable justification, the university may convert its classification of these Digital Data from Category-I Digital Data to a lesser classification upon request by the Data Owner, with appropriate review and approval.

5.9. Risk Management

- 5.9.1. Under the guidance of the Information Security Office, the university shall conduct and document an information security risk assessment annually in accordance with 1 TAC 202.72 that identifies Category-I Digital Data in the central and all decentralized areas.
- 5.9.2. Information Resources must be protected based on sensitivity and risk.
- 5.9.3. The confidentiality, integrity, and availability needs of Digital Data must be managed as required by this Policy.
- 5.9.4. Data not otherwise deemed Category-I must be managed according to the appropriate minimum security standards and policies and, in the case of Research Data, according to federal guidelines for the responsible conduct of Research.

5.10. Reduction of Use and Collection of Social Security Numbers

Information Resources Use and Security Policy

Document Version: Approved

- 5.10.1. The university recognizes the special risks associated with the collections, use, and disclosure of social security numbers. Accordingly, the requirements of this section to apply to all social security numbers contained in any medium, including paper records that are collected, maintained, used, or disclosed by the university.
 - 5.10.1.1. The university shall discontinue the use of social security numbers 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.
 - 5.10.1.2. If the collection and use of social security numbers is permitted, but not required, by applicable law, the university shall use and collect social security numbers only as reasonably necessary for the proper administration or accomplishment of their respective business, governmental, educational and medical purposes, including, but not limited to:
 - 5.10.1.2.1. As a means of identifying an individual for whom a unique identification number is not known;
 - 5.10.1.2.2. For internal verification or administrative purposes; and
 - 5.10.1.2.3. Use for verification or administrative purposes by a third party or agent conducting business on behalf of the university, where the third party or agent has contracted to comply with the safeguards described in [Section 11](#) of this Policy.
 - 5.10.1.3. Except in those instances in which the university is legally required to collect a social security number, an individual shall not be required to disclose his or her social security number and shall not be denied access to the services at issue based on such a refusal. An individual, however, may volunteer his or her social security number. Any request by the university 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 the purposes of this Policy. Examples of federal and state laws that require the collection of 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 Information Security Officer (via security@utexas.edu) who will consult with the Office of Legal Affairs and/or the UT System Office of General Counsel with respect to the interpretation of law.
 - 5.10.1.4. The university reserves the right to designate only selected offices and/or positions as authorized to request that an individual disclose his or her social security number.

- 5.10.1.5. The university shall assign a unique identifier (for example, the UT EID) 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 university.
- 5.10.1.6. The unique identifier shall be used in all electronic and paper Information Systems to identify, track, and serve these individuals. The unique identifier shall:
 - 5.10.1.6.1. Be a component of a system that provides a mechanism for the public identification of individuals;
 - 5.10.1.6.2. Be permanent and unique with the university as applicable and remain the property of, and subject to the rules of, the university; and
 - 5.10.1.6.3. 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 number.
- 5.10.1.7. All services and Information Systems should rely on the identification services provided by the university's unique identifier system.
- 5.10.2. The university shall inform individuals when it collects social security numbers.
 - 5.10.2.1. Each time the university 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. sec. 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.
 - 5.10.2.1.1. The notice shall use the applicable test 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 Legal Affairs and/or the UT System Office of General Counsel with respect to the interpretation of law.
 - 5.10.2.1.2. 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.
 - 5.10.2.1.3. 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 must include the notice printed on the form.

Information Resources Use and Security Policy

Document Version: Approved

- 5.10.2.2. 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 university 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 the 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.
- 5.10.3. Employees may not seek out or use social security numbers relating to others for their own interest or advantage.
- 5.10.4. The university must reduce the public display of social security numbers.
- 5.10.4.1. Grades may not be publicly posted or displayed in a manner in which all of any portion of either the social security number or the unique identifier identifies the individual associated with the information.
- 5.10.4.2. The social security number may not be displayed on documents that can be widely seen by the general public (such as time cards, rosters, 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.
- 5.10.4.3. If the university 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.
- 5.10.4.4. The university shall prohibit employees from sending social security numbers over across a network unless the connection is encrypted end-to-end or the social security number is encrypted or otherwise secured. The university shall require employees sending social security numbers by fax to take appropriate measures to protect the confidentiality of the fax (such measures include confirming with the recipient that the recipient is monitoring the fax machine).
- 5.10.4.5. The university shall not print or cause the 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 university.
- 5.10.5. All Information Systems acquired or developed after January 30, 2004 must comply with the following:

- 5.10.5.1. 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;
- 5.10.5.2. 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;
- 5.10.5.3. 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
- 5.10.5.4. For those databases that require social security numbers, the databases may automatically cross-reference between social security numbers and other information through the use of conversion tables with the Information System or other technical mechanisms.

5.11. Management of Sensitive Digital Data

- 5.11.1. The [Minimum Security Standards for Systems](#) describe and require appropriate steps to protect Category-I Digital Data (for example, social security numbers, protected health information, sensitive research data, digital data associated with an individual and/or digital data protected by law) stored, processed, or transmitted on the university's computing devices.
- 5.11.2. The university shall control and monitor access to its Category-I 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.
 - 5.11.2.1. The university shall limit access to records containing Category-I Digital Data to those employees who need access to the Data for the performance of the employee's job responsibilities.
 - 5.11.2.1.1. Employees may not request disclosure of Category-I Digital Data if it is not necessary and relevant to the purposes of the university and the particular function for which the employee is responsible.
 - 5.11.2.2. The university shall monitor access to records containing Category-I Digital Data by the use of appropriate measures as it reasonably determines.
 - 5.11.2.3. Employees may not disclose Category-I Digital Data to unauthorized persons of entities except:
 - 5.11.2.3.1. As required or permitted by law;
 - 5.11.2.3.2. With the consent of the individual;

Information Resources Use and Security Policy

Document Version: Approved

- 5.11.2.3.3. Where the unauthorized person is the agent or contractor for the university and the safeguards described in Section 11.2.4 are in place to prevent unauthorized distribution; or
- 5.11.2.3.4. As approved by the Office of Legal Affairs or by UT System Office of General Counsel.
- 5.11.2.4. If the university intends to provide Category-I Digital Data to a third party acting as an agent of or otherwise on its behalf (such as an application service provider) and if it determines that its provision of Category-I Digital Data to a third party will result in a significant risk to the confidentiality and/or integrity of such Data, a written agreement with the third party is required. The agreement must specify terms and conditions that protect the confidentiality and/or integrity of the Category-I 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/or integrity of all Category-I Digital Data obtained and that the university, as applicable, shall monitor compliance with the provisions of the written agreement.
 - 5.11.2.4.1. The appropriate university official (for example, the Purchasing Office, Office of Sponsored Projects, or Office of Legal Affairs) must review such written agreements prior to approval.
- 5.11.3. The university shall implement security safeguards to protect its Category-I Digital Data. Such safeguards shall be appropriate to the confidentiality and/or integrity needs of the Digital Data to be protected based on the risk, and in the case of Research Data, the research project requirements for that Category-I Digital Data.
 - 5.11.3.1. Category-I Digital Data shall be secured in accordance with the university's data protection standards and with this Policy.
 - 5.11.3.2. The university shall protect the security of records containing Category-I Digital Data during storage using physical and technical safeguards (such safeguards may include encrypting electronic records, including backups, and locking physical files.)
 - 5.11.3.3. Unless otherwise required by federal or state law or regulation, Category-I Digital Data must not be stored, processed, or transmitted on university or non-university owned computers or other electronic devices (for example, laptop, hand-held device, Flash drive, or other portable computing devices) unless:
 - 5.11.3.3.1. It is secured against unauthorized access in accordance with this Policy;
 - 5.11.3.3.2. It will not compromise business or Research efforts or privacy interests if lost or destroyed; and

5.11.3.3.3. The university has specific procedures in place that address this subsection.

5.11.4. The university shall discard electronic media (for example, disks, tapes, hard drives, etc.) containing Category-I Digital Data as follows:

5.11.4.1. In a verifiable manner that adequately protects the confidentiality of the Category-I Digital Data and renders it unrecoverable, such as modifying the electronic media to make it unreadable or indecipherable or otherwise physically destroying the electronic media; and

5.11.4.2. In accordance with the university's [Records Retention Schedule](#).

5.11.5. The university shall, based on risk, implement all appropriate technical safeguards necessary to adequately protect the security of Category-I Digital Data during electronic communications or transmissions.

5.12. Electronic Mail (E-mail)

5.12.1. E-mail is an essential tool for communicating within the university. It is important that unimpeded e-mail services be available at all times and that e-mail be used in a manner that achieves its purpose without exposing the university to unnecessary technical, financial, or legal risks. The following practices are required:

5.12.1.1. Each faculty member, staff, or student assigned a university e-mail address shall exercise prudent e-mail use in accordance with the policies, standards, and/or procedures related to Information Resources acceptable use and retention.

5.12.1.2. All e-mail is subject to logging and review.

5.12.1.3. To reduce spam and protect the e-mail environment from malicious viruses, worms, or other threats, Information Technology Services (ITS), or an otherwise appropriate department, may filter, block, and/or strip potentially harmful code from e-mail messages.

5.13. Incident Management

5.13.1. Incidents involving computer security will be managed by the Information Security Office and will be reported as required by federal or state law or regulation.

5.13.2. The Information Security Office is required to establish and follow Incident Management Procedures to ensure that each incident is reported, documented and resolved in a manner that restores operation quickly and if required, maintains evidence for further disciplinary, legal, or law enforcement actions.

Information Resources Use and Security Policy

Document Version: Approved

- 5.13.3. All faculty members, staff, and/or students shall report promptly any unauthorized or inappropriate disclosure of Category-I Digital Data, including social security numbers, to: the University Information Security Officer (via security@utexas.edu or 512-475-9242); their supervisors; and/or the university's compliance hotline (via helpline@compliance.utexas.edu or 1-877-888-0002).
- 5.13.4. The University Information Security Officer shall report to the UT System CISO incidents involving computer security that compromise the security, confidentiality, or integrity of Category-I Digital Data or personal identifying information it maintains.
- 5.13.5. The university shall disclose, in accordance with applicable federal or state law, incidents involving computer security that compromise the security, confidentiality, and/or integrity of personal identifying information it maintains to Data Owners and any resident of Texas whose personal identifying information was, or is reasonably believed to have been, acquired without authorization.
 - 5.13.5.1. 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 the 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.
- 5.13.6. The Information Security Office's Incident Management Procedures must incorporate the following:
 - 5.13.6.1. The university will establish a Computer Incident Response Team (CIRT) that, in the event of a significant computer security incident, will initiate and follow the Incident Management Procedures. The members of this team will have defined roles and responsibilities that, based on the severity of the incident, may take priority over normal duties.
 - 5.13.6.2. The University Information Security Officer will report the incident to the appropriate university, state, and federal agencies and departments as required by governing laws, rules, and procedures.
 - 5.13.6.3. The University Information Security Officer, working with the selected Computer Incident Response Team members, will determine if a widespread university communication is required, the content of any such communication, and the method of distribution. The Office of the Vice President for Information Technology and/or the Office of the Vice President for Public Affairs will handle any communications to the general public.

- 5.13.6.4. The University Information Security Officer will be responsible for maintaining a chain of evidence on incidents it investigates, or participates in investigating, in case the incident needs to be referred to law enforcement or other legal proceedings.
- 5.13.6.5. The University Information Security Officer is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation, except in cases involving appropriate law enforcement personnel, where the University Police Department or other law enforcement agencies will make these determinations.
- 5.13.6.6. Technical staff members from the Computer Incident Response Team (CIRT), led by the University Information Security Officer, are responsible for ensuring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized.
- 5.13.6.7. The University Information Security Officer is responsible for communicating new issues or vulnerabilities to vendors as needed, and for working with the vendors to eliminate or mitigate the vulnerabilities.
- 5.13.6.8. The University Information Security Officer is responsible for initiating, completing, and documenting the incident investigation with assistance from the Computer Incident Response Team. The University Police Department serves as liaison with law enforcement organizations.

5.14. Internet Use

- 5.14.1. To mitigate the risks associated with connecting to the Internet, all users of the university's network must adhere to prudent and responsible use practices as outlined in the Acceptable Use Policy and must ensure devices on the university's network comply with the Minimum Security Standards for Systems.
- 5.14.2. Users will adhere to the [Minimum Security Standards for Data Stewardship](#) regarding the secure transmission of Category-I data requiring confidentiality via public networks.
 - 5.14.2.1. Users must encrypt all Category-I Digital Data transmitted over a network unless a specific exception has been filed with the Information Security Office.

5.15. Information Services Privacy

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 the university are not private unless expressly stated by Regent's Rules. They may be accessed as needed for the purpose 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, or other written authorizations, to conduct the business of the university, and to perform audits.

5.16. Network Access

- 5.16.1. All network users are required to acknowledge and abide by all policies relating to the acceptable use of Information Resources.
- 5.16.2. ITS Networking is 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 computer systems or devices to any university network to ensure that access to the network does not compromise the operations and reliability of the network, or compromise the integrity of use of information contained within the network.

5.17. Network Configuration

- 5.17.1. ITS Networking is designated the responsibility for the university's networking infrastructure, which includes all cabling, wireless signaling, and connected electronic devices, to ensure reliability of operations, proper accessibility to resources, and protection of data integrity. ITS Networking is specifically responsible for the following:
 - 5.17.1.1. Operating and maintaining a reliable network with appropriate redundancies to meet quality of service goals.
 - 5.17.1.2. Maintaining a list of systems connected to the university network, ensuring all systems are:
 - 5.17.1.2.1. Registered with the university's domain registrar;
 - 5.17.1.2.2. Associated with a specific university departmental unit;
 - 5.17.1.2.3. Assigned custodian and department head contact information;
 - 5.17.1.2.4. Physically identifiable (such as switch port and room number);
 - 5.17.1.2.5. Identified by service criticality or data classification.
 - 5.17.1.3. Ensuring the Information Security Office regularly scans all systems connected to the university network for high-risk vulnerabilities.
 - 5.17.1.4. Monitoring and identifying network use for operational purposes in accordance with the [Network Monitoring Guidelines](#).
 - 5.17.1.5. Installing or authorizing a contractor to install all cabling and network hardware.

- 5.17.1.6. Approving the specification used to configure all network equipment connected to the university's network.
- 5.17.1.7. Authorizing changes to the configuration of active network management devices.
- 5.17.1.8. Establishing all protocols and standards used on the university's network.
- 5.17.1.9. Operating and managing all connections of the network infrastructure to external third party data and telephony networks.
- 5.17.1.10. Installing, configuring, and maintaining the departmental firewalls in accordance with the Firewall Implementation Standards (forthcoming).
- 5.17.1.11. Providing written authorization for the use of departmental firewalls. Their use is not permitted without written authorization.

5.18. Passwords

Strong passwords shall be used to control access to the university's Information Resources. All account passwords associated with the university's Information Resources must be constructed, implemented, and maintained according to the following, as technology permits:

- 5.18.1. Vetting User identity when issuing or resetting a password;
- 5.18.2. Account passwords must comply with the following password strength requirements:
 - 5.18.2.1. Account passwords associated only with Category-II or \-III data must:
 - 5.18.2.1.1. Be between at least 6 characters in length; and
 - 5.18.2.1.2. Be minimally composed of case sensitive letters and digits.
 - 5.18.2.2. Account passwords associated only with Category-II or \-III data must not:
 - 5.18.2.2.1. Include personal information such as your name, phone number, social security number, date of birth, or addresses; or
 - 5.18.2.2.2. Contain words found in a dictionary
 - 5.18.2.3. Account passwords associated with Category-I data must:
 - 5.18.2.3.1. Be at least 8 characters in length; and
 - 5.18.2.3.2. Contain letters, numbers, and special characters (for example \! @ # \$ % & * () - + = < >)
 - 5.18.2.4. Account passwords associated with Category-I data must not:

Information Resources Use and Security Policy

Document Version: Approved

- 5.18.2.4.1. Include personal information such as your name, phone number, social security number, date of birth, or addresses;
 - 5.18.2.4.2. Contain words found in a dictionary;
 - 5.18.2.4.3. Re-use any of the account's last 10 passwords;
 - 5.18.2.4.4. Contain a series of the same character; or
 - 5.18.2.4.5. Contain the user's account name or respective UT-EID.
- 5.18.3. All password change procedures must include the following:
- 5.18.3.1. Authentication of the user prior to changing the password (acceptable forms of authentication include answering a series of specific questions, showing one or more forms of photo ID, etc.).
 - 5.18.3.2. The new password must comply with password strength requirements associated with the data classification for the service in question.
- 5.18.4. University identity credentials (security tokens, security certificates, smartcards, and other access and identification devices) must be disabled or returned to the appropriate department or entity on demand or upon termination of the relationship with the university. Additional operating guidelines for university ID cards are referenced in the [University Identification Card Guidelines](#) and the [Data Encryption Guidelines](#).
- 5.18.5. Unattended computing devices must be secured from unauthorized access. Physical security options include barriers such as locked doors or security cables. Logical security options include screen saver passwords and automatic session time-outs.

For more information on creating secure "strong" passwords please see the [Password Guidelines](#) published by Information Technology Services.

5.19. Physical Access

- 5.19.1. 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 university.
- 5.19.2. Physical access safeguards help to establish best practices for the appropriate granting, controlling, and monitoring of physical access for all facilities supporting information resources (such as Data Centers). Physical access safeguards include the following:

- 5.19.2.1. All facilities supporting information resources must be physically protected in proportion to the criticality and confidentiality of their function.
- 5.19.2.2. All facilities supporting information resources must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and systems housed in that facility.
- 5.19.2.3. Access to facilities supporting information resources will only be granted to authorized university personnel and other contractors or personnel whose job responsibilities require such action.
- 5.19.2.4. Access cards and/or keys must not be shared or loaned to others.
- 5.19.2.5. Access cards, and/or keys, and badges that are no longer required must be returned to the responsible department contact. All returned access cards must be forwarded to the responsible campus key management or ID center contact as soon as possible. Cards must not be reallocated to another individual, thereby bypassing the return process.
- 5.19.2.6. Lost or stolen access cards and/or keys must be reported to the appropriate department or entity as soon as possible.
- 5.19.2.7. Access and log records for facilities supporting information resources are the responsibility of the department that manages the facility. Such records will be kept in accordance to the accountability requirements of the data and systems in that facility and the university's record retention schedule.
- 5.19.2.8. The department in charge of facilities supporting information resources must be notified within three business days if individuals who had access to these facilities should no longer need access due to a change in roles, completion of contract or other cause that negates their need for further access.
- 5.19.2.9. Visitors must be escorted in controlled areas of facilities supporting information resources.
- 5.19.2.10. The department in charge of facilities supporting information resources must review access records on a periodic basis and investigate any unusual access.
- 5.19.2.11. The department in charge of facilities supporting information resources must review card and/or key access rights on a periodic basis and remove access for individuals that no longer require access.
- 5.19.2.12. Signage for restricted access rooms and locations must be practical. Minimal discernible evidence of the importance of the location should be displayed.

5.20. Portable Computing and Remote Access

- 5.20.1. To preserve the confidentiality, integrity, and availability of university information, Users accessing the university networking infrastructure remotely must do so in accordance with [Sections 2](#) and [11](#) of this Policy and all university policies, standards, and/or procedures regarding acceptable use of Information Resources.
- 5.20.2. [This section to be made effective on December 31, 2011 so as to allow the campus time to transition to the new encryption solution]. Category-I university data stored on portable computing devices introduces serious risk. That risk can be significantly reduced by minimizing the use of portable devices for storage of Category-I data.
- 5.20.2.1. All university owned laptop computing devices must be encrypted, regardless of data classification, using products and/or methods approved by the U.T. Austin Chief Information Security Officer, as detailed on the [Approved Encryption Methods](#) page.
- 5.20.2.1.1. Any Category-I university data stored on other types of university-owned portable devices must be encrypted using native or 3rd party tools approved by the U.T. Austin Chief Information Security Officer. Such portable devices include, but are not limited to, personal digital assistants (PDAs), cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs, magnetic tapes, and similar storage devices.)
- 5.20.2.1.2. Exceptions must be filed with the [Information Security Office](#) in cases where encryption is not possible for any portable device. All exceptions must identify the compensating controls that will be implemented to offset the risk created by the lack of encryption. A single exception may be filed for a number of devices as long as the devices can be uniquely identified (e.g., UT Tag, Serial, MAC address).
- 5.20.2.2. Specific permission must be obtained from the department head before a user may store Category-I university data on any non-university owned portable device. Such permission should be granted only upon demonstration of a business need and an assessment of the risk introduced by the possibility of unauthorized access or loss of the data.
- 5.20.2.2.1. All non-university owned portable devices with a demonstrated business need to store Category-I university data must be encrypted using products and/or methods approved by the U.T. Austin Chief Information Security Officer.

5.20.2.2.2. Exceptions must be filed with the [Information Security Office](#) in the event of hardware compatibility conflicts, technology limitations for certain types of devices, etc. All exceptions must identify the compensating controls that will be implemented to offset the risk created by the lack of encryption. A single exception may be filed for a number of devices as long as the devices can be uniquely identified (e.g., UT Tag, Serial, MAC address).

5.20.2.3. Data owners are responsible for ensuring encrypted data will be accessible in the event decryption keys become lost or forgotten and no other copy of the data is available. Only [escrow methods approved by the U.T. Austin Chief Information Security Officer are permissible](#).

5.21. Security Monitoring

In accordance with [Section 1](#) of this Policy, the university's Information Security Office is charged with securing all network resources, both centralized and decentralized, and has the responsibility and university-wide authority to monitor network traffic and use of Information Resources to confirm that security practices and controls are adhered to and are effective. All security monitoring shall be executed in accordance to the [Network Monitoring Guidelines](#).

5.22. Security Training

5.22.1. The Information Security Office shall deliver security awareness General Compliance training in accordance with the following schedule:

5.22.1.1. Training of all Users, including students, with access to the university's Information Resources shall take place biennially;

5.22.1.2. 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 university or (b) otherwise engaged or assigned to perform such work.

5.22.2. The Information Security Office shall develop required technical training for employees providing information technology help-desk or technical support. This training will include a certification program designed to evaluate job-role skill competencies.

5.23. System Hardening

Systems are used to process and transmit information and services throughout the university. Information and services must be processed and transmitted securely and reliably to assure that data confidentiality, integrity, and availability are preserved.

5.23.1. All systems must be installed and maintained in accordance with the Minimum Security Standards for Systems to minimize service disruptions and prevent unauthorized access or use.

- 5.23.2. The Information Security Office shall provide specific [Hardening Checklists](#) for common operating system platforms and devices.

5.24. Software Licensing

All software used on university computers will be used in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious violation subject to disciplinary action and any such use is without the consent of the university.

- 5.24.1. The university will provide a sufficient number of cost-effective, licensed copies of core business software to enable faculty members, staff, and students to perform their work in an expedient and effective manner.
- 5.24.2. Systems administrators have the right to remove software from university computers for cause. For example, if a user is unable to show proof of license, or if the software is not required for university business purposes, or causes problems on the university-owned computer.
- 5.24.3. All departments or individuals managing university-owned computers will periodically audit all computers to inventory and document all installed software.
- 5.24.4. All departments are responsible for the accurate accounting of software purchased by the department and must ensure that the installation of the software complies with the license agreement of the software. For audit purposes, departments must maintain proof of purchase and/or original installation media for each software package.

5.25. Secure Development and Administration

- 5.25.1. The university 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. The following procedures are required:
 - 5.25.1.1. All associated systems and applications must restrict access and must provide methods for appropriately restricting privileges of authorized users. Access to applications is granted on a need-to-access basis.
 - 5.25.1.1.1. All applications processing Category-I data must comply with the [Minimum Security Standards for Application Development and Administration](#).
 - 5.25.1.2. Separate production and development environments will be maintained to ensure the security and reliability of the central production system. Whenever possible, new development or modifications to a production system will be made first in a development test environment. These changes should be thoroughly tested for valid functionality before being released to the production environment.

- 5.25.2. Information technology outsourcing contracts must address security, backup, and privacy requirements, and should include right-to-audit or other provisions to provide appropriate assurances that applications and data will be adequately protected. Vendors must adhere to all federal and state laws and Regent's Rules pertaining to the protection of Information Resources and privacy of Category-I Digital Data.

5.26. Vendor Access

Vendors serve an important function in the support of hardware and software and in some cases even the operations of computer networks, servers, and/or applications.

- 5.26.1. Contracts must require that vendors comply with all applicable rules associated with this Policy, practice standards and agreements, and address all federal and state laws to which the university must adhere to ensure that it remains in compliance with such law.

- 5.26.2. The university shall control Vendor access to its Category-I data based on data sensitivity, confidentiality, and risk (as determined in accordance with [Section 9](#) of this Policy) and by use of the following measures:

- 5.26.2.1. The Vendor shall represent, warrant, and certify it will:

- 5.26.2.1.1. Hold all Category-I Data in the strictest confidence;
- 5.26.2.1.2. Not release any Category-I Data concerning a university student unless Vendor obtains the university's prior written approval and performs such a release in full compliance with all applicable privacy laws, including FERPA;
- 5.26.2.1.3. Not otherwise use or disclose Category-I data except as required or permitted by law;
- 5.26.2.1.4. Safeguard Category-I data according to all commercially reasonable administrative, physical, and technical standards (for example, such standards established by the National Institute of Standards and Technology or the Center for Internet Security);
- 5.26.2.1.5. Continually monitor its operations and take any action necessary to assure the Category-I data is safeguarded in accordance with the terms of this Policy; and
- 5.26.2.1.6. Comply with the Vendor Access Requirements that are set forth in this section.

- 5.26.2.2. To the extent that the Category-I Data includes Protected Health Information as defined in 45 CFR sec. 164.501, if required by the university, Vendor shall execute a HIPAA Business Associate agreement in the form required by UT System.

Information Resources Use and Security Policy

Document Version: Approved

5.26.2.3. The university shall require the following from the Vendor:

5.26.2.3.1. If an unauthorized use or disclosure of any Category-I data occurs, the Vendor must provide:

5.26.2.3.1.1. Written notice within one (1) business day after the Vendor's discovery of such use or disclosure; and

5.26.2.3.1.2. All information that the university requests concerning such unauthorized use or disclosure.

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

5.26.2.3.2.1. Return or destroy, as applicable, all Category-I data provided to the Vendor by the university, including all such data provided to the Vendor's employees, subcontractors, agents, or other affiliated persons or entities; or

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

5.27. Right to Monitor

Pursuant to Title 1 Texas Administrative Code sec. 202.75 (7) and to ensure compliance with this Policy and state laws and regulations related to the use and security of Information Resources, the university's Information Security Office has the authority and responsibility to monitor Information Resources in accordance with the Network Monitoring Standards.

5.28. Disciplinary Actions

Violation of this Policy or misuse or destruction of Information Resources can vary in severity and appropriate disciplinary actions should be taken in proportion to the severity of the incident. It is not the role of Information Technology professionals to carry out disciplinary actions as the result of an incident, but it is their role to monitor resources, to identify potential incidents and to bring such incidents to the attention of appropriate university officials. The following guidelines apply:

5.28.1. Suspected incidents involving student, faculty, or staff misuse of Information Resources should be brought to the attention of the Information Security Office.

5.28.2. If an investigation involving review of the content of a faculty member, staff member or student's files is required, written permission will be obtained from the Office of Legal Affairs and other departments, as necessary.

- 5.28.3. If it is determined that a misuse violation has occurred by a student, faculty member, or staff member, the incident should be brought to the attention of the Information Security Office. The Information Security Office will consult with the Office of Legal Affairs, Human Resource Services or Student Judicial Services, as needed, and in the case of criminal violations, the University Police Department.
- 5.28.4. Violations by non-affiliates will be referred to the appropriate authorities. The Office of Legal Affairs may be contacted to provide direction in terms of identifying the appropriate authority.

6. Implementation

This Policy is based on public policy and privacy issues and not on convenience or past practices. Nevertheless, the university 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 Category-I data as required or permitted by applicable law; to create unjustified obstacles to conduct the business of the university and the provision of services to its many constituencies; or to negatively affect the university's commitment to engage in high-quality, innovative research that entails the discovery, retention, dissemination, and application of knowledge in compliance with university policy and state and federal laws and regulations.

Some of the requirements of this Policy have immediate compliance dates and others have delayed compliance dates. The university should implement those requirements with delayed compliance dates in a steady and purposeful manner so that they are fully implemented no later than the specified respective compliance dates. The university shall establish priorities for all systems, processes, and research projects that are out of compliance and shall establish a plan for remediating them.

7. 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

8. Definitions

Definitions can be found in the [ISO Technical and Security Glossary](#) and the [UTS-165](#) policy itself.

9. Revision History

Version	Date	New	Original
	6/27/2011	Section 5.2.2: [This section to be made effective on December 31, 2011 so as to allow the campus time to transition to the new encryption solution].	Section 5.2.2: [This section to be made effective on June 20, 2011 so as to allow the campus time to transition to the new encryption solution].
Information Resources Use and Security Policy	2/25/2011	Converted web page to PDF	No changes
	2/9/2011	Clarified language to bring consistency across policies and standards regarding systems that store, process, or transmit sensitive data, as well as with industry standards and government regulations such as PCI and HIPAA.	<p>8.1. All data owners, data stewards, or designated custodians, shall be responsible for classifying Digital Data processed by systems under their purview based on data sensitivity and risk so that the appropriate security controls can be applied.</p> <p>11.1. The Minimum Security Standards for Systems describe and require appropriate steps to protect Category-I Digital Data (for example, social security numbers, protected health information, sensitive research data, digital data associated with an individual and/or digital data protected by law) stored on the university's computing devices.</p> <p>11.3.3. Unless otherwise required by federal or state law or regulation, Category-I Digital Data must not be stored on university or non-university owned computers or other electronic devices (for example, laptop, hand-held device, Flash drive, or other portable computing devices) unless:</p>

Version	Date	New	Original
	12/15/2010	After being approved by IT Governance, the Internal Audit Committee, and the President, Section 20.2 of the IRUSP was modified to require encryption of all university-owned laptops regardless of their data classification. The policy also now references the Information Security Office's approved encryption methods. [This change to be made effective on June 20, 2011 so as to allow the campus time to transition to the new encryption solution]	20.2. All university and non-university owned portable computing devices storing Category-I university data must also comply with UT System Security Practice Bulletin #1 (SPB-1) .
	8/29/2008	Document republished in new HTML format. Removed compliance dates from sections 8 and 22 as those requirements have been met. In section 5, moved information on auditing the backup and recovery plans to sections 5.1 and 5.2 respectively. Updated all references to the university to conform to the university Style Guide .	Old format was PDF. To receive copies of the archived PDF format, please contact the Information Security Office .

Information Resources Use and Security Policy

Document Version: Approved

Version	Date	New	Original
	11/10/2007	<p>New version published to comply with UTS-165. Major changes in this version are:</p> <ul style="list-style-type: none">• Title changed from IT Security Operations Manual to Information Resources Use and Security Policy to better align with U. T. System UTS-165, which consolidated BPM-53, BPM-66, and BPM-75. The structure of the document has also been changed to better track with UTS-165.• Planned to be added to Handbook of Operating Procedures.• Added roles and responsibilities for university IT resources (Sec 1).• Formalized data classification requirements (Sec 8).• Added Risk Management section (Sec 9).• Added Management of Sensitive Data (Sec 11).• Extended specific network responsibilities (e.g., cabling, wireless signaling) to ITS Networking group to ensure operational availability and compatibility.• Added specific training requirements for all IT support staff (Sec 20).	<p>To receive copies of the archived IT Security Operations Manual, please contact the Information Security Office.</p>

Version	Date	New	Original
	4/5/2007	Added links to newly published, approved supplemental standards and guidelines: * Section 23: Minimum Security Standards for Application Development and Administration. * Section 26: Minimum Security Standards for Data Stewardship	Previously noted that documents were forthcoming.
	4/5/2007	Fixed typo in section 26, #4. "Ensure appropriate backup and retention of that data."	"Ensure appropriate backup and retention of that data, and"
	3/28/2007	Changed references from "ITS Telecommunications and Networking" to "ITS Networking." Changed reference in section 6 from "Data Classification Guidelines" to "Data Classification Standard" to reflect correct document title. Corrected typo in section 12.3	"ITS Telecommunications and Networking." "Data Classification Guidelines" "The University"...
	11/20/2006	Changed references from "Data Classification Guidelines" to "Data Classification Standard" to reflect correct document title.	"Data Classification Guidelines"
	10/20/2006	Numbered individual standards within each category for easier reference.	New.
	10/20/2006	Section 12.5, replaced "Information Technology Services" with Information Security Office."	"All confidential, personally identifiable, protected health information, certain financial data, or certain student data transmitted over any network must be encrypted in accordance with Data Classification Guidelines published by Information Technology Services."

Information Resources Use and Security Policy

Document Version: Approved

Version	Date	New	Original
	10/20/2006	Section 14, replaced "ITS" with Information Security Office."	To ensure compatibility with The University of Texas at Austin network, all computers, PDAs and office productivity software purchased by The University of Texas at Austin should adhere to system standards endorsed by ITS.
	10/20/2006	Section 15.3, moved bullet 3 to follow the bulleted list.	"All registered hosts attached to the university network may be scanned by the Information Security Office for potential vulnerabilities." incorrectly appeared within bulleted list.
	10/20/2006	Corrected an indentation problem in Section 16.	"All remote users must comply with the Minimum Security Standards for Systems as published by Information Technology Services."
	10/20/2006	In Section 19.6, removed "ITS" from sentence.	"Any security issues discovered will be reported to the ITS Information Security Office and appropriate executive officials (see Section 25)."
	10/20/2006	Section 20, Replaced "Information Technology Services" with Information Security Office" where appropriate. Removed "(training to be arranged by Information Technology Services)." Security awareness training has been developed by the Information Security Office and is now available through the Compliance Office.	"Recurring security awareness training for all faculty and staff will be offered annually (training to be arranged by Information Technology Services)."
	10/20/2006	In Section 20.7, removed "ITS" from sentence.	"The ITS Information Security Office is responsible for communicating new issues or vulnerabilities to vendors as needed, and for working with the vendors to eliminate or mitigate the vulnerabilities."
	10/20/2006	Changed the title of Section 23 to "Secure Development and Administration."	"Enterprise Development and Deployment."

Version	Date	New	Original
	10/20/2006	Section 24, reworded subsections 4.a, 4.e, and 4f to make more clear.	<ul style="list-style-type: none"> • The University of Texas at Austin information the vendor may access. • The University of Texas at Austin, or respective department, right to audit and otherwise verify the security of university information and other resources in the possession of or being managed by the vendor and the university's right to investigate any security breaches involving these resources. • The University of Texas at Austin, or respective department, right to require background checks for vendors working with security sensitive university information.
	10/20/2006	Corrected typo in section 25.3.	"If it is determined that a misuse violation has occurred by a student, faculty, or staff member, this should be brought to the attention of the Information Security Office. The Information Security Office with consult with either the Human Resource Services or Student Judicial Services, as needed, and in the case of criminal violations, the University Police Department."
	10/20/2006	Added Section 26, "Sensitive Data Classification."	New.
	7/11/2006	Changed title to "IT Security Operations Manual" in this and all documents referencing the title.	"Information Technology Resources Security Operations Manual."
	7/11/2006	Rearranged Change Log to list most recent changes first.	New.
	5/2/2006	Sec. 18: Added link to Minimum Security Standards for Systems.	"All remote users must comply with the Minimum Security Standards for Desktop and Portable Computing as published by Information Technology Services (forthcoming)."

Information Resources Use and Security Policy

Document Version: Approved

Version	Date	New	Original
	3/13/2006	Changed reference from System Hardening Procedure to "Minimum Security Standards for Systems."	"System Hardening Procedure"
	2/20/2006	Added link to Security Exception Request form.	"(forthcoming)"
	1/20/2006	Removed inline glossary and referred to ISO Technical and Security Glossary and Usage Guide . Various corrections to language errors, acronym use, and references. Added "Last reviewed" and "Last updated" dates. Added links to newly published supporting documents.	None.
	12/13/2005	Sec. 25: Added "Issues of departmental non-compliance may be reported to the respective executive management, the Office of Internal Audit, or the Office of the President."	None.
	12/13/2005	Sec. 7, paragraph 1: Added "The following change management procedures are required in proportion to the respective data classification category, the availability requirements of the data, and the impact of the change on the user community:"	"The following change management procedures are required:"
	10/31/2005	Sec. 5: Corrected form name to "Security Sensitive" form, per ISO office.	"Position of Special Trust form."

10. Approvals

Name	Role	Members	Date
Chief Information Security Office	Approval	Cam Beasley	March 3, 2011