UT Tyler Information Security Policies

Policy Statement

1. Overview

1.1 The information assets of The University of Texas at Tyler (UT Tyler) must be administered in conformance with applicable laws and The University of Texas System Board of Regent's Rules and Regulations. Appropriate security controls will be applied based on risk as determined by the potential impact and likelihood of disruptions to the organization's mission, assets, and reputation. This Policy defines UT Tyler organizational expectations for responsible use of UT Tyler Information Systems by building a culture of information security risk awareness and mitigation.

2. Authority

2.1. UT Tyler must comply with information security requirements defined by applicable federal and state regulations, UT System policies, and contractual obligations. This includes Texas Administrative Code 202 (TAC 202), University of Texas System 165 (UTS 165), Texas Medical Records Privacy Act, Texas Public Information Act, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Gramm–Leach–Bliley Act (GLBA), and Digital Millennium Copyright Act (DMCA).

3. Definitions (alphabetical order)

3.1 **Confidential Data:** The subset of University Data that is private or confidential by law or otherwise exempt from public disclosure (i.e. Social Security Numbers, personally identifiable Medical and Medical Payment information, Driver's License Numbers and other governmentissued identification numbers, Education Records subject to the Family Educational Rights & Privacy Act (FERPA), financial account numbers, and/or other University Data about an individual likely to expose the individual to identity theft).

3.2 **Controlled Data:** The subset of University Data that is not created for or made available for public consumption but that is subject to release under the Texas Public Information Act or other laws (i.e. network diagrams, UT Tyler emails, and/or UT Tyler -ID number).

3.3 **Decentralized IT:** UT Tyler employees who report to the heads of business units, departments, or programs and who manage a subset of UT Tyler Information Systems.

3.4 **Incidental Use:** Occasional personal use of UT Tyler Information Systems. Activities related to official duties on behalf of UT Tyler, such as research and teaching, are not Incidental Use.

3.5 **Information Security Standards:** Documented controls specified for specific technology components which, when implemented, reduce risk of compromise (i.e. change default passwords, disable unnecessary services, apply current compatible patches, include in backup scheme)

3.6 **ISO:** Information Security Office is the UT Tyler department, led by the Information Security Officer, assigned responsibility for promoting confidentiality, integrity, availability, and accountability of information assets.

3.7 **Mobile computing device:** Laptops, tablets, smart phones, or other devices designed to be easily portable that are capable of creating, storing, or processing University Data.

3.8 **IT:** Information Technology is the UT Tyler department, led by the Chief Information Officer, assigned responsibility for planning and ongoing operation of centrally-provided information systems such as telecommunications networks, computers, software, databases, system integration and hosted solutions.

3.9 **CCS:** Campus Computing Services the UT Tyler department, led by the Chief Information Officer, assigned the responsibility to providing desktop support to UT Tyler faculty, staff, and students.

3.9 **Published Data:** The subset of University Data intended for public consumption (i.e. marketing materials, press releases, public websites, published papers, and/or UT Tylerissued email address).

3.10 **University Data:** This Policy uses the term University Data to refer to data for which UT Tyler has a responsibility for ensuring appropriate information security or would be liable for data exposure, as defined by applicable law, UT System policy, regulations, or contractual agreements. University Data may include information held on behalf of UT Tyler or created as a result and/or in support of UT Tyler business (i.e. financial records, personnel records, officially maintained student records, and/or records of official UT Tyler committees), including paper records. This definition does not imply, address, or change intellectual property ownership.

3.11 **User:** Any individual granted access to UT Tyler Information Systems, including guests and contractors.

3.12 **UT System:** The University of Texas System

3.13 **UT Tyler:** The University of Texas at Tyler

3.14 **UT Tyler Information Systems:** All computer and telecommunications equipment, software, data, and media, owned or controlled by UT Tyler or maintained on its behalf.

4. Roles & Responsibilities

4.1 Appropriate levels of information security can only be achieved with a well-coordinated team effort across the UT Tyler organization. Stakeholders must work together to identify risks and take responsibility for appropriate controls.

4.2 ISO: The ISO promotes compliance and transparent discussion of risks associated with UT Tyler

Information Systems. The ISO has oversight responsibility including establishing the Information Security and Acceptable Use Policy and related Information Security Standards, testing for compliance, and reporting risk posture to internal and external stakeholders.

4.3 Data Owners (DO): The DO is typically the responsible manager of a school or department that collects or is the primary user of a data asset. DOs are responsible for achieving compliance with this Policy, applying for exemptions when justified, and accepting residual risk when security threats cannot be further mitigated. DO responsibilities include approving or denying requests to access their data and periodically reviewing access assignments and taking corrective action if inappropriate access is detected.

4.4 Information Security Administrator (ISA): An ISA is an individual typically designated by the DO to implement information security policies and procedures and for reporting incidents to the ISO. The ISO performs an annual risk assessment and identifies, recommends, and documents risk levels for information resources under his/her authority.

4.5 Data Custodian (DC): The DC is designated by the DO and assists with the ongoing operational tasks of managing information assets. For example, server and application administrators and software developers may be considered DCs.

4.6 Data User (DU): DUs are the individuals who the DOs authorized to access a data asset. DUs typically have no role in determining the security requirements for the information asset or performing server or application maintenance. Nonetheless, DUs must understand and abide by the security requirements of the information asset and the expectations of the DO and this Policy.

5. Data Classification

5.1 All University Data is subject to a risk-based data classification standard maintained by the ISO and must be protected accordingly. Classifications are Confidential data, Controlled data, and Published data. Definitions of these classification types can be found in sections 3.1, 3.2, and 3.0 of this policy.

5.2 Data classification is the primary factor for establishing necessary security controls. Additional controls may be warranted for systems where integrity, availability, and/or accountability requirements are more critical than the requirements for confidentiality.

6. General

6.1 UT Tyler Information Systems are provided for the purpose of conducting the business of UT Tyler and/or UT System. However, Users are permitted Incidental Use as defined in section 3.4 and detailed in section 8 of this policy.

6.2 Users have no expectation of privacy when using UT Tyler Information Systems except as otherwise provided by UT Tyler’s Privacy Policy and applicable privacy laws. UT Tyler has the authority and responsibility to access and monitor UT Tyler Information Systems for purposes consistent with UT Tyler’s duties and mission.

6.3 University Data created or stored on a User’s personally owned computers, mobile computing devices, removable storage devices, or in databases that are not part of UT Tyler’s Information

Systems are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to UT Tyler Information Systems.

6.4 Users shall never use UT Tyler Information Systems to deprive access to individuals otherwise entitled to access University Data, to circumvent UT Tyler information security measures; or, in any way that is contrary to UT Tyler's mission(s) or applicable law.

6.5 Users may not intentionally deny access to designated administrators of UT Tyler Information Systems.

6.6 Users may be required to complete training on information security, specific to their role in the organization.

6.7 Users should report misuse of UT Tyler Information Systems or violations of this policy to their management, to the ISO, or via the Compliance Hotline.

7. Confidentiality & Security of Data

7.1 Users shall access University Data only to conduct UT Tyler business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access.

7.2 Users shall not disclose Confidential Data or Controlled Data except as permitted or required by law and only as part of their official duties on behalf of UT Tyler.

7.3 Confidential Data or other information essential to the mission of UT Tyler should be stored on a UT Tyler-managed network server when possible, rather than on a UT Tyler-owned desktop workstation, laptop, or portable device.

7.4 Users are encouraged to store any University Data on UT Tyler Information Systems, rather than personally owned equipment.

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

7.6 Confidential Data must be encrypted during transmission over any network. Users will be provided with tools and processes to encrypt confidential data to be sent over the network.

7.7 Users may not store University Data with a third party storage service (often referred to as "cloud" storage) unless the service has been sanctioned by the University.

7.8 Users must not use security programs or utilities except as such programs that are required to perform their official duties on behalf of UT Tyler.

7.9 The ISO may temporarily limit or disable network connectivity for devices that pose a significant threat to UT Tyler Information Systems or University Data.

7.10 UT Tyler Information Systems may be monitored by ISO and/or IT personnel responding to an investigation or incident, at the direction of UT Tyler's President, UT Tyler Human Resources, UT Tyler or UT System Counsel, and/or law enforcement; or at the direction of UT Tyler Office of Administration when processing requests made in accordance with the Texas Public Information Act.

8. Incidental Use of UT Tyler Information Systems

8.1 Incidental Use of UT Tyler Information Systems must not interfere with User's performance of official UT Tyler business, pose an unreasonable burden on system resources, result in direct costs to UT Tyler, expose UT Tyler to unreasonable risks, or violate applicable laws or other UT Tyler or UT System policy.

8.2 Users should use personally owned systems, rather than UT Tyler Information Systems, for conducting personal computing and must understand that personally owned content stored on UT Tyler Information Systems may be visible to UT Tyler personnel whose job responsibilities involve the management and monitoring of UT Tyler Information Systems.

8.3 A User's Incidental Use of UT Tyler Information Systems does not extend to the User's family members or others regardless of physical location.

8.4 Incidental Use may include communications such as e-mails, web pages, and social media posts; if such communications could be reasonably interpreted as expressing the opinion or position of UT Tyler, they should be accompanied by a disclaimer (i.e. "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas at Tyler").

8.5 Incidental Use to conduct or promote the User's outside employment, including selfemployment, is prohibited unless such use is approved by the User's dean or department head.

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

8.7 Accessing, creating, storing, or transmitting sexually explicit materials during Incidental Use is prohibited. Questions regarding whether particular content is "sexually explicit material" should be directed to UT Tyler counsel or the UT System Office of General Counsel.

9. Email

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

9.2 Users are expected to use UT Tyler-provided email accounts for conducting UT Tyler business, rather than personal email accounts; Users are encouraged to use personal email accounts for conducting personal communication and business, rather than UT Tyler-provided email accounts.

9.3 When using UT Tyler-provided email accounts to create accounts with third parties to conduct UT Tyler business, users should never use identical or similar passwords that they use to logon to UT Tyler owned servers.

9.4 Emails containing Confidential Data must be encrypted with tools and processes approved by the ISO in order to reduce risk of interception.

9.5 The following email activities are prohibited when using a UT Tyler-provided email account:

9.5.1 Sending an email under another individual's name or email address, except when authorized to do so by the intended User of the email account for a work-related purpose.

9.5.2 Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of UT Tyler.

9.5.3 Maliciously sending or forwarding any email that is suspected by the User to contain computer malware. Forwarding to a malware researcher or ISO for analysis does not represent malicious intent.

9.5.4 Any Incidental Use prohibited by this policy.

9.5.5 Any use prohibited by applicable UT Tyler or UT System policy.

10. Portable and Remote Computing

10.1 All electronic devices, including personally owned computing devices used to access, create or store Confidential Data or Controlled Data, must be protected by mechanisms (i.e. passwords or biometrics) that limit access to authorized Users, in accordance with UT Tyler Information Security Standards.

10.2 All UT Tyler-issued mobile computing devices must be encrypted.

10.3 Any personally owned computing devices on which Confidential Data is stored or created, including desktops, laptops, tablets, smartphones, or externally hard drives, must be encrypted in a manner which protects the Confidential Data from unauthorized access.

10.4 University Data created and/or stored on personal computers, other computing devices and/or non-UT Tyler Information Systems should be transferred to UT Tyler Information Systems as soon as feasible.

10.5 Because portable computers, smart phones, and other computing devices are targets for theft, Users are expected to take reasonable precautions to physically secure UT Tyler Information Systems or personally owned computing devices containing University Data.

10.6 All remote access to Confidential Data and Controlled Data must be accomplished using an encrypted method approved by ISO (i.e. VPN, SSH, and/or Outlook Web Access).

11. Access Control

11.1 Individuals provided with a system account shall securely maintain and never disclose their credentials or knowingly permit another individual to access UT Tyler Information Systems via his/her account, except in accordance with a lawful investigation. Any individual who knowingly accesses UT Tyler Information Systems with a user account not specifically assigned to him/her is in violation of this Policy.

11.2 Employees whose job duties require accessing UT Tyler computing devices will be assigned a username and password. In rare instances, a shared account may be created when the account is justified by the functions being performed. Accounts designed specifically for a shared purpose or specific system task will be granted only in cases when absolutely necessary, and will only be shared with the individuals performing UT Tyler operations.

11.3 Computing accounts providing access to UT Tyler Information Systems will only be created when necessary to achieve UT Tyler objectives. Access privileges will be assigned to provide the minimum necessary permission to perform job responsibilities.

11.4 UT Tyler Information Systems are subject to risk-based authentication configuration settings defined in Information Security Standards (i.e. password length, complexity, and 2-factor authentication).

11.5 Account credentials should not be hard coded into scripts, software code, or system configurations. When hard coding credentials is deemed necessary, system owners will store these files in a secure manner and will maintain sufficient documentation to allow periodic manual changes to passwords or other credentials.

11.6 Users requesting local admin rights to a workstation must be able to demonstrate a business need in order for access to be granted. The request should be submitted to CCS by the user's supervisor, and requires the approval of both the supervisor, and the manager of CCS. The ISO may remove local admin rights from a user's workstation when there is a reasonable indication that the elevated rights pose a risk to the UT Tyler network, data, services, or servers.

11.7 ISO will administer an annual account sponsorship renewal process, whereby accounts will be verified by responsible management and disabled if no longer necessary or associated with a valid User at UT Tyler.

11.8 When employment relationships are subject to change or termination, responsible management will participate in checkout processes defined by Human Resources to ensure timely disabling of system access.

11.9 In order to limit the possibility of malicious access, the ISO may disable computing accounts based on reasonable indication that the account has been disclosed to, or compromised by, a malicious third party. ISO shall assist in re-establishing control of the account to the intended User.

11.10 UT Tyler Information Systems access should be designed to maintain separation of duties to reduce the risk of a malicious individual performing conflicting activities. Compensating controls such as log monitoring and system-enforced thresholds may also be implemented when conflicting duties cannot be separated.

12. Computer Systems Security

12.1 All UT Tyler Information Systems, including production and non-production systems, must be configured and operated in accordance with Information Security Standards.

12.2 All UT Tyler Information Systems should be updated with the latest compatible software patches. This includes patches for the operating system and third-party applications. Highpriority patches may need to be installed outside of routine change control procedures at the request of the ISO in order to address critical security vulnerabilities.

12.3 The ISO may participate at key steps of projects involving access to Confidential Data or Controlled Data. ISO should assess security controls and notify stakeholders of risks prior to introducing new solutions into production. Costs of security testing, if applicable, will be considered part of the project budget.

12.4 All paid for and free software should be reviewed and approved by Technology Support or the Information Security Office before being installed on University owned devices. This includes renewals and add-ons to software that has already been purchased and approved prior to the add-on being purchased.

12.5 Software installed by users that could potentially impede security, or other operational functions in the campus computing environment, will result in the workstation being disconnected from the campus network and the software being removed from the workstation.

13. Data Destruction

13.1 Data must be stored and retained according to the UT Tyler Records Retention Schedule. To prevent access to Confidential Data by unauthorized parties, storage media must be destroyed according to Information Security Standards.

13.2 Storage media (i.e. hard drives, flash memory, magnetic data tapes, and floppy disks) must be securely overwritten before reuse and physically destroyed at the end of the useful life of the device.

13.3 Paper and CD/DVD optical media must be securely shredded in a manner sufficient to prevent reassembly.

13.4 UT Tyler-issued mobile computing devices should be surrendered to the ISO to have an electronic erase or factory reset procedure performed before the device is issued to another User, or retired from service.

13.5 All hard drives, external drives, thumb drives, and mobile devices should be surrendered to the ISO to have all UT Tyler data erased before being disposed of.

13.5 Vendors who host data remotely must provide UT Tyler with a certificate of data destruction upon termination of the contract.

14. Physical Security

14.1 Locations that support access to UT Tyler Information Systems must be protected in accordance with value of the information assets at risk. High-risk locations include, but are not limited to, data centers, server closets, wiring closets, file rooms, and research labs.

14.2 Users are encouraged to wear UT Tyler identification in restricted access areas; visible UT Tyler identification may be required at the discretion of a dean or department head.

14.3 Users who work in restricted access areas should remain aware of unidentified individuals who may attempt to gain access.

14.4 Locked doors protecting restricted access areas should not be propped open if unattended.

14.5 Users will maintain a workspace where Confidential Data or Controlled Data is stored in a manner to mitigate risk of observation or theft by unauthorized parties (i.e. locked offices, locked file cabinets, and/or privacy screens).

15. Third-Party Vendors

15.1 All vendors that host or access University Data must be pre-approved by the Information Security Office prior to use and are subject to a risk assessment performed by the ISO. This includes acquisition (paid or free) and use of external services such as cloud storage, application or communication providers.

15.2 Contracts with third parties will include expectations for information security.

15.3 Third parties will be expected to protect UT Tyler Information Systems and University Data with security equal to or better than levels defined in this Policy and applicable Information Security Standards.

15.4 All third parties performing tasks or data processing for UT Tyler are required to notify UT Tyler immediately if a security incident has occurred, or is suspected to have occurred.

16. Exemptions

16.1 Compliance with all elements of this policy may not be possible in some situations given the tradeoffs between risk, cost, and operational impact. Users may request exemptions to elements of this Policy; requests will be subject to approval or denial by the ISO within 30 days of the request. When applicable, DOs will be asked to accept risks associated with noncompliance. Exemption requests should include an explanation of why compliance with specific Policy elements is not feasible and should describe compensating controls that are in place to reduce risk. Approved exemptions will include an expiration date and be tracked by the ISO.

16.2 Exemption requests not approved by the ISO may be appealed to UT Tyler's President.

17. Disciplinary Actions

17.1 Instances of noncompliance, or attempted noncompliance, may constitute a security violation that is subject to investigation and possible disciplinary action, civil prosecution, and/or criminal prosecution in accordance with applicable policies and laws.

17.2 Violations may result in disciplinary action by Human Resources in accordance with pertinent policies, up to and including termination of work relationships. Students involved in violations will be referred to the Office of Student Affairs. Suspected illegal activities will be escalated to appropriate law enforcement agencies.

17.3 This Policy does not create or supersede any existing UT Tyler processes for taking disciplinary action. The ISO, which shall not take direct disciplinary action against a User, will participate in existing UT Tyler processes for taking disciplinary action.

18. Acceptable Use

18.1 Per UTS-165, all institutions within UT System must have an Acceptable Use Policy. By acknowledging this Information Security and Acceptable Use Policy, users are acknowledging policies for Acceptable Use.

19. User Acknowledgement

19.1 Users must acknowledge that they received and read the Information Security and Acceptable Use Policy. They must understand and agree that use of UT Tyler Information Systems is conditioned upon agreement to comply; noncompliance may result in disciplinary action as outlined above.