TEXAS TECH UNIVERSITY
INFORMATION SECURITY PLAN FOR FINANCIAL INFORMATION

1. Introduction

This Information Security Plan ("Plan") describes Texas Tech University (TTU)'s safeguards to protect *covered data and information*.[1] These safeguards are intended to:

- Promote security, integrity, and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security, integrity, or confidentiality of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any individual who has provided covered data and information.

This plan also provides mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by TTU;
- Develop written policies and procedures to manage and control these risks;
- Implement and review this plan; and
- Adjust this plan to reflect changes in technology, the sensitivity of covered data and information, and internal or external threats to information security.

2. Identification and Assessment of Potential Risks to Covered Data and Information

TTU recognizes that there are both potential internal and external risks. These potential risks include, but are not limited to:

- Unauthorized access of covered data and information:
    - By someone other than the owner of the covered data and information;
    - By TTU employees or affiliates;
    - Through hardcopy files or reports;
- Unauthorized requests for covered data and information;
- Unauthorized transfer of covered data and information through third parties;
- Compromised system security;
- Interception of data during transmission;
- Loss of data integrity;
- Loss of system integrity;

[1] *Covered data and information*, for the purposes of this plan, means *nonpublic personal information* that is obtained from *financial activities* and that is required to be protected under the Gramm-Leach-Bliley Act (GBLA) of 1999, 15 U.S.C. 6801, *et seq.*, implemented by 16 CFR Part 314. For definitions of *nonpublic personal information* and *financial activities*, refer to 16 CFR 313.3(n), 16 CFR 313.3(o), and 12 USC 1843(k). *Nonpublic personal information* includes, but is not limited to, the awarding and issuance of student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of personal information could include addresses, phone numbers, bank and credit card account numbers, income and credit histories, payment histories, and Social Security numbers, in both paper and electronic format. However, the Federal Educational Rights and Privacy Act of 1974 does allow for disclosure of "directory information" in certain circumstances (34 CFR Part 99).

- Physical loss of data in a disaster; and
- Errors introduced into the system.

TTU recognizes that this may not be a complete list of the potential risks associated with the protection of covered data and information. Since technology growth is not static, new risks may occur periodically. Accordingly, the Information Technology Division of TTU will actively participate and monitor advisory groups such as the Educause Security Institute, SANS, and the Department of Information Resources of the state of Texas for identification of new risks.

TTU Information Technology Division's current safeguards are reasonable and sufficient to provide security and confidentiality to covered data and information maintained by TTU. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

3. Information Security Plan Coordinators (16 CFR 314.4(a))

a. Coordinators

The area heads of Administration and Finance, including Fiscal Affairs; Human Resources; Enrollment Management; Texas Tech University System Office of Institutional Advancement (those offices located at TTU); Information Technology (chair); Texas Tech University System Information Technology; Student Affairs; and any other areas that work with covered data and information on a regular basis (collectively referred to hereinafter as the "coordinators") are responsible for coordination and execution of this plan. With consultation from the Office of General Counsel when necessary, the coordinators are responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to TTU.

b. Correspondence and Inquiries

Correspondence and inquiries regarding this plan should be directed to:

Information Technology Policy and Planning Officer
Box 42008
Lubbock, Texas 79409
806-742-5151

4. Design and Implementation of Safeguards Program (16 CFR 314.4(b)-(c))

a. Employee Management and Training

TTU areas that are covered by this policy are Administration and Finance, including Fiscal Affairs; Human Resources; Enrollment Management; Texas Tech University System Office of Institutional Advancement (those offices located at TTU); Information Technology; Texas Tech University System Information Technology; Student Affairs (at all campuses); and any other areas that work with covered data and information on a regular basis. Reference verification and a security background check for potential new employees working in these areas shall be conducted, in accordance with OP 70.20, Employment For Security-Sensitive Positions. New employees in said areas will receive training on the importance of confidentiality of student, faculty, and staff records and financial information, and other types of covered data and

information. TTU also will train current employees working in these areas on the importance of confidentiality of covered data and information. Department administrators will be responsible for ensuring that all employees within their respective areas receive the training required under this policy.

Training of new and current employees working in these areas will include controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "social engineering,"[2] and how to properly dispose of documents that contain covered data and information. All new employees, whether or not they are in an area responsible for maintaining covered data and information, will receive general training in the proper handling and use of covered data and the use of computer information and passwords. Texas Tech will maintain records of employee training. Training materials will be reviewed annually and updated when necessary.

Each area responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss, or damage due to environmental hazards, such as fire and water damage or technical failures. Faculty, staff, students, and affiliates, prior to employment will complete a *Confidentiality Agreement* (Attachment A) and a *Student Records Confidentiality Agreement* (Attachment B) (if the person will have access to the Student Information System), as required by TTU OP 70.40. Department administrators are responsible for ensuring that all employees within their respective areas complete the required confidentiality statements and that the statements are forwarded to the appropriate department for placement in the permanent personnel file as required by TTU OP 70.40.

b. Physical Security

TTU has addressed the physical security of covered data and information shall be accessed only by those employees who have a business reason to know such information. For example, personal customer information, accounts, balances, and transactional information are available only to TTU employees with an appropriate business need for such information.

Loan files, account information, and other paper documents are kept in file cabinets, rooms, or vaults that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain covered data and information shall be shredded at the time of disposal and disposal shall be in compliance with OP 10.10, Records Retention.

c. Information Systems

Access to covered data and information via TTU's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information including, but not limited to, accounts, balances, and transactional information are available only to TTU employees in appropriate departments and positions.

[2] Social engineering (such as *Phishing or pretext calling)* occurs when an individual improperly obtains personal information of TTU customers to be able to commit identity theft. It is accomplished by contacting TTU, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of TTU to release customer identifying information.

Passwords used to authenticate user ids must be changed in accordance with Information Technology security policies and meet the minimum password requirements set by the Information Technology Division.

TTU will take reasonable and appropriate steps consistent with current technological developments to secure all covered data and information and to safeguard the integrity of records in storage and transmission. The Information Technology Division requires that all users comply with Texas Tech University Information Technology Security Policies, thereby allowing the Information Technology Division to verify that the system access meets necessary security requirements. These requirements include maintaining the operating system and applications, including application of appropriate patches and updates in a timely fashion. User and system passwords are also required to comply with the TTU password requirements. In addition, an intrusion prevention system, as well as other security infrastructure, has been implemented to detect and prevent certain threats, along with an incident response plan for occasions where intrusions do occur.

Encryption technology will be utilized for both storage and transmission of covered data and information in accordance with Texas Tech University Information Technology security policies, which are available at http://www.infotech.ttu.edu/security.

In order to protect the confidentiality of privileged and/or sensitive information, any e-mail or fax correspondence that contains Social Security numbers, student information, or any personal and/or confidential information shall contain a disclaimer at the end of the e-mail or cover page of the fax indicating that the information is confidential. Refer to Email Policy (https://www.depts.ttu.edu/infotech/security/docs/email.php) for confidentiality disclaimer recommended by the TTU IT Division and the Office of the General Counsel. Additionally, TTU IT security policies require confidential or sensitive information transmitted over an external network to be encrypted.

d. Management of System Failures

The Information Technology Division has developed written plans and procedures to detect any actual or attempted attacks on TTU systems and has an incident management policy, which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This policy is available upon request from the TTU IT policy and planning officer.

e. Reviews

Areas maintaining covered data and information (with assistance, if necessary, from the coordinators, Office of Audit Services, and/or Office of General Counsel) will be responsible for conducting annual reviews of their respective areas to assess the internal control structure and to verify that their areas are in compliance with requirements and applicable state and federal laws. The Office of Audit Services may conduct reviews of areas maintaining covered data and information at any time and at the discretion of the Office of Audit Services.

5. Selection of Appropriate Service Providers (16 CFR 314.4(d))

It may be necessary for service providers to access covered data and information and provide resources that TTU determines not to provide on its own. In the process of choosing a service

provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. In addition to the standard contract clauses, contracts with service providers shall include the following provisions:

- An explicit acknowledgement that the contract allows the service provider access to confidential information held or collected by TTU and any access to TTU's data/facility/computer system must be approved and coordinated through the TTU Information Security officer. No automated tools may be installed by contract provider without prior authorization from the TTU Office of the CIO;
- A specific definition or description of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- An assurance from the service provider that the provider will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;
- A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract and destruction of that information to be provided by the contract provider to TTU;
- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles TTU to terminate the contract immediately without penalty; and
- A provision stating that the contract's confidentiality requirements shall survive termination.

6. Continuing Evaluation and Adjustment (16 CFR 314.4(e))

This information security plan will be subject to periodic review and adjustment by the coordinators. The most frequent of these reviews will occur within the Information Technology Division, where constantly changing technology and evolving risks mandate increased vigilance. Information Technology, Administration and Finance, and Enrollment Management, as well as other relevant areas, will conduct an annual data and information security review. Continued administration of the development, implementation, and maintenance of the plan will be the responsibility of the coordinators who will assign specific responsibility for implementation and administration as appropriate. The coordinators, in consultation with the Office of General Counsel when necessary, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

7. Corrective Action

To enforce this plan, TTU may take appropriate corrective measures directed to TTU faculty, staff, students, or affiliates consistent with Texas Tech University policy, up to and including termination of employment.