TEXAS TECH™

Operating Policy and Procedure

**OP 70.40: Information Privacy and Confidentiality Statements**

**DATE:** August 14, 2024

**PURPOSE:** The purpose of this Operating Policy/Procedure (OP) is to establish procedures and safeguards for the protection of all information made confidential by law or TTU policy.

**REVIEW:** This OP will be reviewed every two years after publication by the Associate Vice President for Human Resources, the Chief Information Officers, the Assistant Vice President and Chief Procurement Officer, and the Vice Chancellor and General Counsel with substantive revisions presented to the Vice President for Administration and Chief of Staff.

## POLICY/PROCEDURE

### 1. General Policy

a. Anyone who has access to confidential and/or personally identifiable information concerning university faculty, staff, students, affiliates, or others, including donors or vendors, or who has access to any information made confidential by TTU policies or law (including, but not limited to the Family Educational Rights and Privacy Act of 1974 and the Gramm-Leach-Bliley Act of 1999), will take reasonable and necessary steps to ensure the privacy of such information.

(1) For the purposes of this OP, "access" is defined as "any person who has been given an account to access any TTU-provided information system, regardless of location or method of access."

(2) "Confidential and/or personally identifiable information" includes, but is not limited to, social security numbers, birth dates, driver's license numbers, unpublished home addresses or phone numbers, personal account numbers, usernames, passwords and accounts, protected health information (e.g., patient records and information), and financial information.

b. Each department administrator, within their respective area of responsibility, shall be responsible for notifying faculty, staff, students, and affiliates, or others, including vendors and certain donors, of the requirements of this policy and shall be responsible for scheduling faculty, staff, and students for any training required under the provisions of this policy and shall be responsible for ensuring that such training has been completed.

c. All faculty, staff, and student employees are required to sign a *Confidentiality Statement* (Attachment A) and a *Confidentiality of Student Information Systems Records Agreement*

(Attachment B) during their new hire onboarding process. The properly executed statements will become a permanent part of the employee record, as appropriate.

d. As part of the purchasing requisition process (TechBuy), the requesting department is responsible for notifying Procurement Services of any privacy or confidential information risks with vendors on the *Contract Routing Sheet* or the *Intended Use of Technology Form*, as appropriate, including, but not limited to, social security numbers, birth dates, driver's license numbers, unpublished home addresses or phone numbers, personal account numbers, usernames and passwords, R#s, protected health information (e.g., patient records and information), student data, and financial information. Procurement Services will assist the department in negotiating a contract with the vendor that mitigates the risks and ensures proper procedures and liability of the vendor.

e. Certain donors identified by the TTU Office of University Advancement or the Texas Tech University System (TTUS) Office of Institutional Advancement as eligible to access confidential donor information in conjunction with serving on advisory or governing boards or other committees shall be required to sign a *Confidentiality Statement* (Attachment A). *Confidentiality Statements* will be maintained by Legal Counsel for the TTUS Office of Institutional Advancement and disposed of in accordance with OP 10.10, Records Retention. Donors shall not have access to student records unless access is a part of their normal job function as described in paragraphs c or d above.

f. Use or disclosure of any financial information that is covered by any state or federal financial regulation or law, including, but not limited to, the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. 6801, et. Seq., implemented by 16 C.F.R. Part 314, FTC Red Flag Rules, etc., shall be governed by the TTU *Information Security Plan for Financial Information* (Attachment C). "Financial information" includes, but is not limited to, information obtained in connection with the award and issuance of student aid and billing.

g. With the exception of those parts of this policy governed by other TTU operating policies/procedures, responsibility for ensuring the implementation of and compliance with this policy shall rest with the Provost and the vice presidents within their areas of responsibilities.

## 2. Departmental Safeguards

Each department is responsible for establishing procedures necessary to implement this OP. When appropriate, departments should utilize the following practices to protect confidential and/or personally identifiable information.

a. General

Each department must maintain records listing employees who have access to files with sensitive information and the names of the types of files to which they have access.

b. Printed Copies

Use – Records containing confidential and/or personally identifiable information must be secured when not in use; e.g., the records may be locked in a desk drawer or filing cabinet.

Disposal – When discarding documents containing confidential and/or personally identifiable information, use cross-cut shredders or a comparable method designed to ensure privacy. Disposal must be in accordance with OP 10.10, Records Retention.

c. Electronic Data

Persons with access to electronic data containing confidential and/or personally identifiable information should take adequate steps to ensure that such information is not captured by, used by, accessible to, or released to unauthorized sources or unauthorized information technology systems. When deleting files containing such information, the files should be securely deleted so that the information contained in the files cannot be recovered.

d. Review of Departmental Processes

A department should be aware of the types of information being gathered within the department such as sign-in sheets, forms of identification, retrieval and use of records, and posting/storing of information. A department should determine the necessity of obtaining confidential and/or personally identifiable information and revise processes where appropriate.

e. Remote Access

Remote access to sensitive/confidential TTU information is subject to all applicable TTU OPs and IT security policies and procedures, including, but not limited to, the Remote Access Security policy.

f. Third Party Release of Information

Each department should also evaluate the potential risk for misuse when releasing any confidential and/or personally identifiable information to any internal or external third party.

g. Other

Safeguarding confidential and/or personally identifiable information should not be limited to the above categories. Changing technologies or laws may make additional safeguards necessary.

## 3. Reporting Violations

a. Administration, faculty, staff, or students at TTU who know of or suspect a violation of this policy shall report that incident promptly to their immediate supervisor, the appropriate department administrator, the Registrar, or, when appropriate, in accordance with the TTU *Information Security Plan for Financial Information* and/or OP 52.04, Information Technology (IT) Security. In cases where the immediate supervisor is the known or suspected violator, employees shall report the known or suspected violation to the next higher administrative supervisor.

b. All information acquired in the investigation of any known or suspected violation of this policy shall be confidential unless disclosure is authorized by law.

## 4. Corrective Action

a. Employees

Employees (faculty, staff, or student employees) found to be in violation of this policy will be subject to corrective action up to and including termination and may be subject to additional legal action.

The procedures set forth in TTU OP 70.31, Employee Conduct, Coaching, Corrective Action, and Termination, shall apply to non-faculty employees.

The procedures set forth in OP 32.04, Conduct of University Faculty; OP 32.02, Faculty Non-reappointment, Dismissal, and Tenure Revocation; and Sections 04.03 and 04.04, *Regents' Rules* shall apply to faculty employees.

b. Students

For the purpose of this policy, "students" refers to all students enrolled at TTU, TTUHSC, or an affiliated institution who, as part of their curriculum, attend or participate in classes at TTU. Additional policies and procedures concerning students are set forth in the TTU *Student Handbook*.

c. Affiliates

For the purposes of this policy, "affiliates" refers to volunteers or other non-student or non-employee individuals working in TTU facilities. Violation of this policy will result in loss of privileges, removal from institutional facilities, and possible legal action in accordance with the terms of the contract.

## 5. Authoritative References

Texas Government Code, Section 552.002

*Regents' Rules*, Section 04.03 and 04.04

Family Education Rights and Privacy Act

Gramm-Leach-Bliley Act

## 6. Right to Change Policy

Texas Tech University reserves the right to interpret, change, modify, amend, or rescind this policy, in whole or in part, at any time without the consent of employees.

Attachment A: *Confidentiality Statement*

Attachment B: *Confidentiality of Student Information System Records Agreement*

Attachment C: *Information Security Plan for Financial Information*