TEXAS TECH UNIVERSITY

Operating Policy and Procedure

OP 52.01: Information Technology (IT) Operations

DATE: July 15, 2022

PURPOSE: The purpose of this Operating Policy/Procedure (OP) is to establish policies regarding information technology operations and resources at Texas Tech University (TTU).

REVIEW: This OP will be reviewed in November of even-numbered years by the Associate/Assistant Vice President(s) for IT and the Senior Director of IT Policy & Planning who will recommend substantive revisions to the TTU Chief Information Officer (CIO).

POLICY/PROCEDURE

1. All faculty, staff, students, and other authorized users of TTU IT resources are responsible for complying with this policy on information technology operations and all other applicable policies regarding the use of TTU IT resources, including the Acceptable Use policy (https://www.depts.ttu.edu/infotech/security/docs/acceptable_use.php).

2. All TTU information technology infrastructures are managed by the TTU Office of the CIO. No other areas, departments, or individuals may duplicate, modify, build, add, or attach to the IT infrastructure without explicit approval from the TTU CIO. (Examples of IT infrastructure include, but are not limited to, the following: logical and physical data and video networks over wired and wireless connections, video conferencing, email, security, network-based virtualization services, enterprise systems, authentication, and data center operations.) The Telecommunications department will coordinate projects with Physical Plant in accordance with OP 61.12, Installation of Cabling in Buildings, Tunnels, and Other TTU Locations.

3. Per Texas statutes, TTU information resources* are strategic assets of the State of Texas that must be managed as valuable state resources.†

   a. Use of functional mailboxes is required when provisioning services such as subscriptions, departmental social media accounts, etc. to ensure the strategic management and continuation of the service for the university in the event of personnel changes. Non-TTU email addresses are not allowed for use when conducting university business.

   b. Use of TTU information resources is subject to university OPs and other applicable laws. Unauthorized use is prohibited, usage may be subject to security testing and monitoring, misuse is subject to criminal prosecution, and users have no expectation of privacy except as otherwise provided by applicable privacy laws.‡

4. In accordance with Texas Administrative Code § 202 and Texas Government Code § 2054:

* As defined by Texas Government Code § 2054.003(7)
† Mandated by Texas Government Code § 2054.001(a)(1)
‡ Mandated by Security Controls Standards Catalog AC-8

a. All TTU employees must complete cybersecurity online training annually.

b. All designated area and department IT staff must complete the online cybersecurity training for IT professionals annually.

c. Any service provider with access to a state computer system or database must complete an annual cybersecurity training program provided by TTU. For the purposes of this section,

(1) the term "service provider" has the same meaning as "contractor" and includes subcontractors, officers, or employees of the service provider;

(2) the term "access" is defined as "any person who has been given an account to access any State (or local) information system."

5. Procurement of Information Resources

a. All procurement of information resources equaling or exceeding $10,000 is subject to review and approval by the TTU CIO. This includes, but is not limited to, equipment, hardware, software, and professional services.

(1) Deliverables such as a website or mobile app that processes sensitive information or personally identifiable information (PII) or confidential information must have had a recent vulnerability scan and penetration test conducted (i.e., within the last two years.)[§] Additional review may be conducted, as needed.

(2) This review does not include Library electronic subscriptions and materials if the access or security protocols are the same as the established protocols in place as those previously reviewed and approved by the TTU Information Security Officer.

b. Any procurement of information resources requiring system integration with institutional enterprise information systems must be reviewed and approved by the TTU Office of the CIO prior to implementation.

c. All procurement of Internet/cloud computing services, IT security services, and networking equipment/supplies, regardless of cost, are subject to review and approval by the TTU CIO.

(1) Pursuant to Texas Government Code § 2054.0593(d)–(f), beginning January 1, 2022, TTU may only enter into or renew contracts that involve cloud computing services (as defined by Texas Government Code § 2157.007) in any capacity with vendors that are listed on DIR's TX-RAMP list.

(2) Cloud computing services vendors must comply with the requirements of TX-RAMP and maintain their compliance and certification throughout the term of the contract.

6. All procurement of telecommunications equipment and services will be in accordance with OP 52.03, Telecommunications Services.

[§] Mandated by Texas Government Code § 2054.516

7. Any contract involving data sharing/transfer of TTU data must be reviewed and approved by the TTU Office of the CIO prior to implementation.

8. All eCommerce solutions are required to use institutional payment gateways and are subject to review and approval by the TTU CIO, per OP 62.06, Payment Card Processing by University Departments. Any exceptions must be approved by the TTU Office of the CIO.

9. All electronic and information resources (EIR) must comply with the accessibility requirements outlined in OP 52.05, Electronic and Information Resources Accessibility. (Electronic and information resources include information technology and any equipment or interconnected systems or subsystem of equipment that is used in the creation, conversion, duplication, storage, or delivery of data or information.[**])

10. To expedite evaluation and the procurement process, departments should contact the TTU Office of the CIO early in the decision-making process, prior to submitting procurement documents.

11. TTU departments, employees, and contractors must take reasonable and necessary steps to ensure privacy of student education records, personally identifiable information (PII), protected health information (PHI), and other confidential or sensitive information at TTU. For information regarding information privacy and confidentiality, see OP 70.40, Information Privacy and Confidentiality Statements.

a. All institutional data that is classified as Confidential, Sensitive, Regulated, Mission-Critical, or is otherwise subject to restricted access requirements, must be stored or processed only on information resources located in the University Data Center.

b. PHI data must not be stored on a local workstation or on the TTU network. TTU has an agreement in place with Texas Tech University Health Sciences Center to store PHI used for authorized TTU research projects in their HIPAA-compliant data center, or at other HIPAA-compliant locations approved by the TTU CIO. Contact the TTU Office of the CIO for more information.

c. Requests for access to or copies of TTU information must be reviewed carefully and on a case-by-case basis. Per Texas Tech University System Regulation 07.01, all requests for information must be sent in writing to the Office of General Counsel. This includes requests for access to electronic records.

12. All use of information resources is subject to TTU IT security policies, as referenced in OP 52.04, Information Technology (IT) Security.

13. Use of social media for university business is subject to all applicable TTU IT OPs and policies, including the Acceptable Use policy.

14. Any faculty, staff, or student conduct on personal social media that violates local, state, or federal law or university policy may result in disciplinary action. Human Resources will assist the relevant administrators with addressing issues involving employees. Student Life will review and address issues involving students.[††]

[**] Defined by Texas Administrative Code § 213.1(9)
[††] See TTU OP 52.04 section 9

15. The TTU CIO serves as the Information Resource Manager (IRM) for Texas Tech University, as referenced in the Texas Administrative Code.

16. The TTU CIO appoints the Information Security Officer for the university, as referenced in the Texas Administrative Code. The current Chief Information Security Officer (CISO) for TTU and the TTU System is the Associate Vice President for IT overseeing the IT security operations for the university, unless otherwise designated by the TTU CIO.

17. The TTU CIO appoints the IT Accessibility Coordinator for the university, as referenced in the Texas Administrative Code. The current IT Accessibility Coordinator for the university is the Senior Director – IT Policy & Planning, unless otherwise designated by the TTU CIO.

18. The TTU CIO has final authority on all TTU IT-related issues, including exceptions to existing IT policies.

19. 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 or students.