TEXAS TECH UNIVERSITY™

Operating Policy and Procedure

OP 52.01: Information Technology (IT) Operations

DATE: July 7, 2017

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 Assistant Vice President(s) for IT and the IT Policy and Planning Officer 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.

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 and Tunnels.

3. Per Texas statutes, TTU information resources* are strategic assets of the state of Texas that must be managed as valuable state resources†. As such, 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. All procurement of information resources, including, but not limited to, equipment, hardware, software, and professional services equaling or exceeding $10,000 is subject to review and approval by the CIO. Additional review may be conducted, as needed. To expedite evaluation and the procurement process, departments should contact the TTU Office of the TTU CIO early in the decision-making process, prior to submitting procurement documents.

5. All procurement of Internet/computing services and networking equipment/supplies, regardless of cost, are subject to review and approval by the TTU CIO. To expedite evaluation and the

* 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

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

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

7. 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.

8. All electronic and information resources 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, or delivery of data or information.[§])

9. 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 theTTU Office of the CIO for more information.

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

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

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

13. 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 Managing Director of TTU Technology Support, unless otherwise designated by the TTU CIO.

[§] Defined by Texas Administrative Code §213.1(6)

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

15. 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.