



## TEXAS TECH UNIVERSITY

### Operating Policy and Procedure

#### **OP 52.04: Information Technology (IT) Security**

**DATE:** October 13, 2017

**PURPOSE:** The purpose of this Operating Policy/Procedure (OP) is to establish policies for IT security at Texas Tech University (TTU).

**REVIEW:** This OP will be reviewed in November of even-numbered years by the TTU Information Security Officer, the TTU IT Policy and Planning Officer, and the Office of the General Counsel who will recommend substantive revisions to the TTU Chief Information Officer (CIO).

#### **POLICY/PROCEDURE**

1. All IT security incidents will be reported to and handled by the TTU Information Security Officer (ISO) in the TTU Office of the CIO, or an explicitly directed designee of the CIO.
2. IT security standards and practices at TTU will meet a minimum standard outlined within the Texas Administrative Code, Title 1, Part 10, Chapter 202, Information Security Standards.
3. Information resources<sup>1</sup> are considered critical resources of TTU and must only be used for their intended purposes<sup>2</sup>. Information resources shall be protected with an appropriate level of security<sup>3</sup>. Protection of all TTU data and information resources must meet the minimum standards set forth in the TTU IT security policies. Details of TTU IT security policies are located at <http://www.infotech.ttu.edu/security>.
4. University-owned computer systems must be kept current with critical security updates. Similarly, antivirus software must be enabled and up-to-date with the latest virus definitions on all university-owned computer systems. Specific recommendations and information on safe computing practices for the TTU community are located at <http://www.ttu.edu/cybersecurity/ttu/>.
5. Some jobs or activities at TTU may involve access to resources critical to computer security and privacy (security sensitive positions). TTU may require faculty/staff employees, students, and other authorized users involved in these jobs or activities to participate in special training, sign special agreements concerning computer use, be subject to non-disclosed surveillance of computer use, disclose personal histories, and/or be subject to a pre-employment criminal background check.

---

<sup>1</sup> As defined by Texas Government Code §2054.003(7)

<sup>2</sup> Mandated by Texas Administrative Code §202.72(3)

<sup>3</sup> Mandated by Security Controls Standards Catalog AC-3

6. All faculty, staff, students, and other authorized users are accountable for their actions in the use of any information resources<sup>4</sup> and shall comply with all applicable TTU policies, and local, state, and federal laws.
7. Any faculty, staff, student, or other authorized user involved in infractions of this policy, another TTU policy, and/or civil/criminal laws regarding computer security and privacy will be subject to disciplinary action, which may include revocation of computing privileges, disciplinary leave, demotion, and termination, and may also be subject to criminal prosecution and restitution for damages, regardless of employment contracts or tenure status. Involvement as used here includes participating in, encouraging, aiding, or failing to report known infractions.
8. Violations of TTU IT security policies are grounds for loss of privileges and/or disciplinary action up to and including termination. Violations may also be reported to the appropriate local, state, and/or federal authorities, as appropriate.
9. All personnel and/or disciplinary actions outlined above will be in accordance with [OPs 32.01, Promotion and Tenure Standards and Procedures](#); [32.04, Conduct of University Faculty](#); [32.05, Faculty Grievance Procedures](#); [32.26, Faculty Departure Notification Procedure](#); [70.10, Non-Faculty Employee Complaint Procedures](#); [70.14, Salary Administration Policy](#); [70.20, Employment in Security-sensitive Positions](#); [OP 70.31, Employee Conduct, Coaching, Corrective Action, and Termination](#); and [70.40, Information Privacy and Confidentiality Statements](#); the *Code of Student Conduct*; and Chapters 03, Personnel, and 04, Academic Affairs, of the *Regents' Rules*.
10. When used to access TTU networks, IT services, and/or data, personally-owned computing devices, including but not limited to desktops, laptops, smartphones, and tablets, are subject to all applicable TTU IT Security Policies. In order to protect the integrity of TTU IT infrastructure, services, networks, and to protect TTU data, TTU may implement certain security controls for university-owned and personally-owned devices that may require the use of software and/or specific settings on the devices before being allowed to access university IT resources.
11. The TTU CIO has final authority on all TTU IT-related issues, including exceptions to existing IT policies.

## 12. **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.

---

<sup>4</sup> Mandated by Texas Administrative Code §202.70(3)