Texas Tech University System
Regulation 06.01

Research Security Compliance

Approved: September 1, 2025
Next Scheduled Review: April 2026

1. Purpose

    a. Texas Education Code Section 51.956 requires public institutions of higher education to establish a policy framework for research security. The purpose of this regulation is to outline a system-wide framework for the Texas Tech University System ("System") and its component universities (each a "University") to implement policies and procedures that promote secure academic research while mitigating the risks of foreign espionage and interference.

    b. This regulation establishes minimum standards for compliance with Texas Education Code Section 51.956 research security requirements. This regulation applies to all TTUS component institutions, including Texas Tech University (TTU), Texas Tech University Health Sciences Center (TTUHSC), Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso), Angelo State University (ASU), and Midwestern State University (MSU).

2. Policy Statement
    a. TTUS is committed to safeguarding research integrity by implementing security protocols, ensuring compliance with all legal and regulatory requirements, and minimizing risks of foreign interference.

    b. This regulation establishes (or facilitates) alignment with the National Defense Authorization Act (NDAA), Controlled Unclassified Information (CUI) standards, and the prohibition on participation in Maligned Foreign Talent Programs.

3. Research Security Framework

The Texas Tech University System Research Security Framework is structured to provide centralized oversight, guidance, and support while enabling component universities to execute research security practices within their specific operational contexts.

a. System-Level Responsibilities

i. The System Research Security Officer (RSO) serves as the primary coordinator of research security efforts across all component universities. The RSO is responsible for maintaining compliance with federal regulations, including Controlled Unclassified (CUI) guidelines, and overseeing classified information management.
ii. The System has established standardized research security policies, including restrictions on participation in Maligned Foreign Talent Programs. These policies are disseminated to all component universities and are updated as required by changes in legislation or regulatory guidance.
iii. The RSO conducts periodic system-wide risk assessments, focusing on foreign influence risks, classified research, and data security. Findings are used to develop targeted mitigation strategies implemented across the component universities.
iv. The System provides annual research security training for faculty, staff, and researchers to address compliance requirements, reporting responsibilities, and best practices for mitigating research risks. Customized training modules are made available to meet the specific needs of individual universities.

b. Component University Responsibilities

i. In compliance with Texas Education Code 51.956, each component university shall submit for Board of Regents approval a policy framework for research security that addresses efforts to achieve applicable compliance standards, promoting an organizational culture of compliance with federal requirements and designating a person within each component to be responsible for maintaining classified information, maintaining controlled unclassified information, conducting foreign influence reporting and addressing other issues at the specific institution associated with the underlying goals of this regulation. The component may satisfy the requirements of the individual appointment through the designation of the research security liaison as discussed below.
ii. Each component university will designate a Research Security Liaison (RSL) to coordinate with the System RSO. The RSL is responsible for ensuring adherence to System policies, reporting compliance concerns, and disseminating training materials to their respective campus communities.
iii. Each component university shall use an approved platform for managing CUI, export controls, and classified research. All research projects shall be reviewed for compliance with export control and foreign influence policies prior to approval.
iv. Each component university is required to report security breaches, foreign influence concerns, or research security compliance violations directly to the System RSO within 24 hours of identification.

c. System-Wide Tools and Resources

    i. A centralized Research Security Portal will be maintained to facilitate incident reporting, document management and policy updates.
    ii. The System RSO provides Universities with tools for conducting localized risk assessments of research projects and personnel.
    iii. Regulation communication between the System RSO, RSLs, and University leadership ensures alignment of research security practices and timely resolution of compliance issues.

d. Monitoring and Review

    i. The System RSO, in collaboration with System Audit, will conduct regular audits of research security practices at each component University. Findings are presented to the Chancellor and appropriate University President, along with recommended improvements.
    ii. The System RSO and RSLs shall collaborate to review research security trends and update policies and practices accordingly.

e. Reporting and Accountability

    i. The System RSO shall compile an annual research security report summarizing compliance activities, risk mitigation outcomes, and training initiatives. This report shall be submitted annually to the Board of Regents.

Contact Office: TTU Office of Research & Innovation
806-834-0705