TENNESSEE STATE UNIVERSITY

Research Security Policy

Policy No. 530

Effective Date: January 1, 2025

I. INTRODUCTION

Tennessee State University (TSU) is committed to maintaining the integrity, transparency, and security of its research enterprise. This Research Security Policy outlines principles, practices, and requirements designed to safeguard TSU's academic and intellectual resources against undue foreign influence, insider threats, and cybersecurity risks.

This policy complies with the National Security Presidential Memorandum-33 (NSPM-33), the CHIPS and Science Act (Public Law No: 117-167), the Office of Science and Technology Policy (OSTP) Guidelines for Research Security Programs at Covered Institutions, and T.C.A. § 49-7-188.

The Research Security Program incorporates best practices in research administration, risk management, and regulatory compliance to ensure TSU maintains a secure and productive research environment. This policy applies to all faculty, staff, students, and affiliates involved in TSU research activities, regardless of funding source.

II. PURPOSE

The primary objectives of this policy are to:

- **Protect** TSU's research activities and intellectual property from undue foreign influence and other security threats.

- **Ensure compliance** with federal, state, and institutional laws, regulations, and guidelines.

- **Promote a culture** of research security awareness and compliance among faculty, staff, and students.

- **Facilitate transparency** in disclosures, training, reporting, and monitoring processes.

III. SCOPE

This policy applies to all individuals engaged in research under the auspices of TSU, including faculty, staff, students, contractors, and other affiliates.

IV. DEFINITIONS

A. Conflict of Interest (“COI”). A situation where a financial or personal relationship has the potential to influence or appear to influence research decisions or outcomes.

B. Conflict of Commitment (“COC”). A situation in which external professional or personal activities interfere with an individual’s responsibilities to TSU.

C. Covered Individual**.** Any TSU faculty, staff, student, or affiliate involved in research activities under TSU’s auspices.

D. Export Control. U.S. regulations that govern the transfer of certain materials, technologies, and data to foreign countries, entities, or individuals.

E. Foreign Country of Concern. Countries identified by the U.S. Department of State as posing risks to national security.

F. Insider Threat. A potential risk posed by an individual with authorized access to institutional resources who may misuse this access.

G. National Security Presidential Memorandum-33 (“NSPM-33”). A directive establishing guidelines for research security at federally funded institutions.

H. NIST Cybersecurity Framework. A set of standards and best practices for managing cybersecurity risks.

I. Public Chapter No. 955. A Tennessee state law addressing research security at public institutions.

V. RESPONSIBLE OFFICIAL

A. The Chief Research Officer shall be responsible for:

1. Maintaining publicly accessible contact information for this policy.

2. Ensuring the distribution of communications on research security matters concerning the University’ academic research enterprise, including any research involving the University.

3. Ensuring compliance with this policy and all policies, procedures, and guidelines developed hereunder.

4. Coordinating and overseeing University research security risk assessment and monitoring programs.

5. Advising and coordinating research security training, reviews, and program implementation.

6. Referring research security incidents to the appropriate University programs for review and implementing resolution decisions.

7. Corresponding with governmental authorities as needed and in coordination with other University personnel.

8. Maintaining a website and other appropriate communication initiatives concerning this policy.

9. Certifying University compliance with governmental research security program requirements.

VI. PROCEDURES

A. Disclosures to Federal Research Funding Agencies

Covered Individuals must fully disclose:

- Foreign affiliations, collaborations, and support.
- Outside appointments and activities.
- Financial interests and resources that directly or indirectly supporting research.

Disclosures will adhere to all applicable requirements of federal agencies, including, but not limited to, those outlined in NSPM-33 and the CHIPS and Science Act. Noncompliance may result in disciplinary action, including, but not limited to, suspension of research privileges or other University discipline.

B. Conflict of Interest and Conflict of Commitment

1. Conflict of Interest (COI**).** Covered Individuals must disclose financial interests or relationships that may influence, or appear to influence, research outcomes.

2. Conflict of Commitment (COC**).** External professional obligations must not interfere with a Covered Individual's primary responsibilities to TSU.

TSU will provide training and establish review processes to identify, mitigate, and manage COI and COC matters and to ensure compliance with federal and OSTP guidelines.

C. **Cybersecurity**

To protect sensitive research data, TSU implements a comprehensive cybersecurity framework aligned with the NIST Cybersecurity Framework:

- Multi-factor authentication ("MFA") for system access.
- Encryption of sensitive data during storage and transmission.
- Regular vulnerability assessments and security updates.
- Mandatory cybersecurity training for all research personnel.

Researchers must report cybersecurity incidents promptly to TSU's IT Department.

D. **Foreign Travel Security**

All TSU personnel traveling internationally for research purposes must:

- Submit travel plans for review and approval by the TSU Office of Research Security.
- Complete mandatory foreign travel security and export control training.
- Adhere to federal and institutional guidelines for transporting research data, materials, and devices.

Foreign travel will be monitored to ensure compliance with institutional and federal regulations. Covered Individuals must cooperate in good faith and in a timely manner with all requests concerning foreign travel.

E. **Research Security and Insider Threat Awareness Training**

Annual mandatory training will be provided and will include:

- Recognizing and responding to suspicious activities.
- Best practices for safeguarding research data and materials.
- Reporting procedures for security threats.

Training will align with NSPM-33 and OSTP requirements to enhance resilience against insider threats and any other training as may be designated by the Chief Research Officer.

F. Export Control Training

To comply with U.S. export control regulations, including International Traffic in Arms Regulations ("ITAR") and Export Administration Regulations ("EAR"), Covered Individuals must:

- Complete export control training if their work involves controlled technologies or data.
- Consult with the Chief Research Officer before transferring materials or information outside the U.S.

Failure to comply with export control laws may result in penalties, including criminal charges.

G. Reporting

All Covered Individuals are required to report:

- Research security incidents, including cyber breaches and unauthorized disclosures.
- Suspicious activities or insider threats.

Reports should be directed to the TSU Office of Research and Sponsored Programs and, where necessary, escalated to federal agencies in accordance with NSPM-33.

H. Implementation and Review

This policy will be reviewed annually by the TSU Office of Research and Sponsored Programs to align with evolving federal and state regulations. Updates and recommendations will be submitted to University leadership for approval.

Additional, relevant TSU research policies can be found at https://www.tnstate.edu/research-1/compliance/policies.aspx.

By adhering to this Research Security Policy, TSU fosters a secure research environment that supports innovation while protecting national security and institutional integrity.

Approved:

Relevant Policies:

https://www.tnstate.edu/research-1/compliance/policies.aspx

https://www.tnstate.edu/facultysenate/handbook.aspx