Institutional Research Security Policy

Policy Name: Institutional Research Security Policy

Policy Purpose

This policy specifies how the institution will safeguard ETSU research and development against interference by U.S.-designated foreign adversaries or any threat to the integrity and conduct of institution's research activities.

Applicability

This policy is applicable to ETSU employees, students, volunteers, guests, and third-party licensees.

Responsible Official, Office, and Interpretation

The Provost is responsible for the review and revision of this policy. For questions about this policy, please contact the Office of the Vice Provost for Research. The Provost, in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Insider Threat

Potential for an individual connected with East Tennessee State University to use their authorized access to or understanding of institutional resources to cause harm to East Tennessee State University. This harm can include, but is not limited to, malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of East Tennessee State University, its data, personnel, or facilities.

Research and Development

Creative and systematic work undertaken to increase the stock of knowledge – including knowledge of people, culture, and society – and to devise new applications using available knowledge. Research and Development includes basic research, applied research, and experimental development.

Policy Effective Date: 12/17/24• **Policy Revised:** Insert
Procedures Effective Date: 12/17/24 • **Procedures Revised:** Insert

Page 2 of 5

Policy Name: Institutional Research Security Policy

U.S.-Designated Foreign Adversaries

Countries, entities, or individuals identified by the U.S. government as posing a threat to national security or the interests of the United States. These adversaries may engage in activities such as espionage, cyber-attacks, or other forms of interference that compromise the integrity of U.S. institutions, technologies, and intellectual property. The designation is typically made by federal agencies, including the Department of State, Department of Justice, Department of Defense, and Department of Commerce.

Policy

East Tennessee State University (ETSU) is committed to safeguarding the University's Research and Development enterprise and adhering to federal, state, and all other applicable legal requirements.

To safeguard Research and Development at ETSU against interference by U.S.-Designated Foreign Adversaries or any threat to the integrity of research conducted by ETSU employees, students, volunteers, guests, and third-party licensees, ETSU will comply with all applicable legal, regulatory, and contractual standards and requirements for securing and protecting the institution's academic research enterprise, including, as applicable, any research involving the institution and its internal components.

A list of U.S.-Designated Foreign Adversaries can be found on U.S. government websites, which are regularly updated. University personnel are encouraged to contact the Office of Research and Sponsored Programs Administration (ORSPA) for the latest information.

The Office of the Vice Provost for Research, in partnership with the Offices of Administration, Business and Finance, Information Technology Services, University Counsel, and the Provost, is responsible for promoting an institutional culture of compliance with the institution's research security policy consistent with federal regulations to ensure that the institution maintains eligibility for federal funding, including, as applicable, federal risk mitigation requirements pertaining to standardized disclosures, cybersecurity, foreign travel security, insider threats, and export controls.

The Vice Provost for Research, or qualified designee, serves as Research Security Officer (RSO) for ETSU. The RSO is responsible for coordinating:

1. The establishment of policies and procedures to ensure compliance with, and reporting within, the institution's research security policy;

Policy Effective Date: 12/17/24• **Policy Revised:** Insert
Procedures Effective Date: 12/17/24 • **Procedures Revised:** Insert

Page 3 of 5

Policy Name: Institutional Research Security Policy

2. The review of the research security policy and procedures to reflect changes in applicable legal and regulatory requirements at a minimum every three years;

3. The communication to the ETSU community regarding research security matters concerning the institution's academic research enterprise;

4. Publicly accessible contact information on the OVPR website; and

5. The establishment of the institution's infrastructure in coordination with other applicable ETSU divisions, offices, and units. The infrastructure will include, but is not limited to, establishing an incident reporting and response program for research security matters.

At a minimum, the incident reporting and response program shall require ETSU employees and researchers to report information that may negatively impact research security and shall establish procedures for resolving research security incidents in coordination with necessary University and campus programs and offices. The incident reporting and response program shall also establish points of contact and communication standards for any required communications with government personnel in relation to research security incidents. Failure to report may result in disciplinary action under the Misconduct in Scholarship and Research Policy, including and up to suspension or termination.

The University Office of Internal Audit shall conduct periodic compliance reviews of the research security policies and procedures every three years with the first review to be conducted before the conclusion of fiscal year 2028.

Policy Effective Date: 12/17/24• **Policy Revised:** Insert
Procedures Effective Date: 12/17/24 • **Procedures Revised:** Insert

Page 4 of 5

Policy Name: Institutional Research Security Policy

Procedures

N/A

Applicable Forms and Websites

[Research Compliance](#)

Authority and Revisions

Authority: TCA § 49-8-203 et seq.; TCA § 49-7-188; National Security Presidential Memorandum-33; CHIPS and Science Act (Public Law No: 117-167); Office of Science and Technology Policy (OSTP) Guidelines for Research Security Programs at Covered Institutions (July 9, 2024)

Previous Policy: N/A

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational program and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the [Policy Development and Rule Making Policy webpage](#).

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.

Policy Effective Date: 12/17/24• **Policy Revised:** Insert
Procedures Effective Date: 12/17/24 • **Procedures Revised:** Insert

Page 5 of 5