Policy Chapter:	**Chapter 13 Research and Innovation**
Policy Number and Title:	**13.020 Research Security**

I. Policy Statement

UNT is committed to the highest standards of integrity to promote responsible research, global engagement, and the protection of sensitive information while ensuring alignment with national security priorities and eligibility for federal research funding. This policy is intended to comply with research security requirements in accordance with the Texas Education Code, which mandates the development of a research security policy framework at all institutions of higher education in the State of Texas and to establish a comprehensive framework to promote secure academic research at UNT while mitigating the risk of foreign espionage and interference.

II. Application of Policy

This policy applies to all faculty, staff, students, postdoctoral researchers, visiting collaborators, and any other individuals engaged in Research Activities at or on behalf of the University. This policy applies regardless of funding source, research location, employment status, or citizenship or nationality. The Vice President for Research and Innovation (VPRI) maintains ultimate institutional authority for research security compliance and shall ensure this policy is implemented across all UNT Research Activities.

III. Policy Definitions

A. Controlled Unclassified Information (CUI)

"Controlled Unclassified Information," or "CUI," in this policy, means information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or government-wide policy, but is not classified.

B. Covered Individuals

"Covered Individuals," in this policy, means an individual who contributes in a substantive, meaningful way to the scientific development or execution of a research project, including principal investigators, co-principal investigators, senior/key personnel, individuals accessing controlled unclassified or export-controlled information, and research security compliance personnel.

C. Classified Information

"Classified Information" or "Classified National Security Information," in this policy, means information that has been determined pursuant to Executive Order (E.O.) 12958 as amended by E.O. 13292, or any successor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form, as identified in NIST SP 800-59 under Classified Information from E.O. 13292.

D. Controlled Environment

"Controlled Environment," in this policy, means any physical area or space and Technology

Environment with adequate physical, technical, administrative, and procedural controls, preventing the unauthorized access or disclosure of Controlled Unclassified Information (CUI).

E. Foreign Adversary Country (FAC)

"Foreign Adversary Country," "FAC," or "Foreign Adversaries," in this policy, are the foreign governments identified in 15 C.F.R. §791.4 that have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons.

F. Intellectual Property (IP)

"Intellectual Property," or "IP," in this policy, means any new and useful process, scientific or technological innovation, technology, machine, composition of matter, life form, article of manufacture, software, tangible property, research data, or any work that is subject to protection by patents, copyrights, trademarks, or trade secrets. It includes such things as new or improved devices, circuits, chemical compounds, drugs, genetically engineered biological organisms, data sets, software, musical processes, unique and innovative uses of existing inventions and any other deemed property. Intellectual Property may or may not be patentable, copyrightable, subject to trade secret, or subject to a trademark.

G. Material Transfer Agreement

"Material Transfer Agreement," in this policy, means a written contract between senders and recipients of research materials that governs the use of the materials.

H. Research Activities

"Research Activities," in this policy, means research projects involving CUI, sensitive or controlled technologies, or potential national security implications; research projects with international collaborations or foreign funding; compliance with security requirements established by funding sources; activities that are subject to export control restrictions; hosting of foreign visitor or visiting collaborators; participation in conferences and workshops; publication of research results; technology transfer; and travel related to any of the aforementioned activities.

I. Research Data

"Research Data," in this policy, means the recorded factual material commonly accepted in the scientific community as necessary to validate research findings, but not any of the following: Preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, or communications with colleagues.

J. Research Security

"Research Security," in this policy, as stated by the National Security Presidential Memorandum-33, is defined as safeguarding the research enterprise against the

misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.

K. Research Security Council

"Research Security Council," or "Council," in this policy, means the Higher Education Research Security Council established in Texas Education Code § 51.957 to promote secure academic research at tier one research institutions while mitigating the risk of foreign espionage and interference.

L. Research Security Office

"Research Security Office," in this policy, means the office responsible for implementing and overseeing research security compliance.

M. Research Security Officer

"Research Security Officer," in this policy, means the individual designated in accordance with Texas Education Code § 51.957(c)(3) responsible for maintaining classified information, maintaining controlled unclassified information, conducting foreign influence reporting, and addressing other research security issues.

N. Research Security Program (RSP)

"Research Security Program," in this policy, is the UNT compliance program charged with adhering to the requirements of the National Security Presidential Memorandum-33 (NSPM-33), classified information, CUI, export control restrictions, Texas Education Code § 51.956, and the accurate and timely completion of all reporting requirements as related to Research Activities.

O. University-Sponsored Travel

"University-Sponsored Travel," in this policy, means any educational or business travel that is UNT-administered, UNT-organized, or conducted within one's capacity as a UNT representative, regardless of credit or funding. University-Sponsored Travel includes:

1. Any faculty, staff, student, visiting collaborator or official guests/volunteers traveling internationally to participate in a UNT-administered or UNT-organized activity or program, or to conduct University business as a representative of UNT.
2. Any event, program, or activity involving international travel that is UNT-administered or UNT-organized. This includes an activity or program to conduct University business as a representative of UNT and includes, but is not limited to:
    a. study abroad programs;
    b. student exchange programs;
    c. class field trips;

d. registered student organization trips;

e. sponsored student organization trips;

f. field studies;

g. research trips;

h. internships or practicums;

i. conferences, seminars, or meetings;

j. teaching endeavors;

k. service-learning opportunities; and

l. volunteer, experiential, or work programs organized, endorsed, or promoted by UNT.

P. UNT Research Security Committee

"UNT Research Security Committee," in this policy, means the committee established under this policy to provide oversight and strategic direction for research security compliance at UNT.

Q. Visiting Collaborator (VC)

"Visiting Collaborator," in this policy, is an individual who is defined as a visiting collaborator under UNT Policy 13.019, Visiting Collaborators.

IV. Policy Responsibilities

A. Administrative Responsibility

This framework is intended to address the research security risk areas applicable to the UNT research portfolio. The Research Security Program (RSP) will have administrative responsibility for the following regulatory and policy areas:

1. Export Control

The university conducts research in accordance with applicable export control laws and regulations.

Laws and regulations promulgated by the U.S. Department of Commerce (EAR), the U.S. Department of State (ITAR), and the U.S. Treasury Department (OFAC) are the bases for restricting use of and access to controlled information, goods, and technology for reasons of national security or protection of trade. The Vice President of Research and Innovation serves as the designated Empowered Official (EO), as defined under 22 CFR § 120.25, and is authorized to make institutional determinations related to export-controlled activities.

All faculty, staff, and students must be aware of and are responsible for the export-

control implications of their work and must ensure that their activities conform to export control laws and regulations. All UNT personnel involved in export-controlled Research Activities must complete export control training prior to the beginning of the Research Activity and annually thereafter.

The principal investigator for a research project has the primary responsibility for compliance. Academic deans, directors, and chairs have responsibility for overseeing export control compliance in their respective schools, departments, centers, or institutes and supporting the Research Security Office and the Export Control Officer in implementing procedures for export control compliance.

Grants and Contract Administration shall review all research projects for potential export control issues prior to initiation. Export Controls are managed through UNT Policy 13.010, Export Controls.

2. Research Security Training and Insider Threat Awareness

The University provides training to researchers, staff, and students to increase their understanding of Research Security principles and best practices and to promote a culture of responsibility and awareness regarding Research Security.

Consistent with the CHIPS and Science Act § 10634 (42 U.S.C. § 19234), UNT requires research security training, including insider threat awareness, for Covered Individuals prior to submitting federal Research and Development award applications.

a. Covered Individuals: Principal investigators, co-principal investigators, senior/key personnel, individuals accessing controlled unclassified or export-controlled information, and research security compliance personnel.

b. Requirements: Initial training prior to federal proposal submission; refresher training every year; event-driven training within 30 days of security incidents; documentation by the Research Security Office.

c. Content: Research security threats, insider threats, foreign interference, disclosure requirements, export controls, cybersecurity, and federal agency-designated topics.

d. Coordination: The Research Security Office shall verify completion prior to proposal submission and maintain records per federal requirements.

3. International Travel Security

The University ensures the safety and security of its students, faculty, staff, and other members of its community when traveling abroad for educational, research, or work-related purposes and has procedures in place to minimize risks of foreign interference.

All faculty, staff, and students participating in international University business or University-Sponsored Travel and initiatives are required to register international travel at least three weeks before departure through Risk Management. Risk Management will inform the Research Security Office of all international travel. All international travelers must complete an International Travel Device Checklist and receive a pre-travel briefing by the Research Security Office.

In accordance with Texas Executive Order GA 48, UNT explicitly prohibits travel to FAC for official University business. Furthermore, Texas Executive Order GA 48 requires faculty and staff who travel to one of the FAC for personal reasons must (1) notify the University prior to travel; and (2) inform the University of the actual travel dates and purpose of the travel upon return. Faculty and staff who travel to one of the FAC for personal reasons are prohibited from conducting University business associated in any way with that country. International Travel is managed through UNT Policy 15.017, International Travel.

4. Foreign Funding and Relationship Reporting

   The Research Security Office serves in an administrative capacity to collaborate with all divisions and units on campus, including the Office of Grants and Contracts, University Advancement, Academic Units, and UNT System Administration, to support reporting requirements to the U.S. Department of Education and the Texas Higher Education Coordinating Board regarding foreign funding and relationships.

   In accordance with Texas Executive Order GA 48, UNT explicitly prohibits contracts, research agreements, financial transactions, or collaborative engagements with entities or individuals considered Foreign Adversaries. The following activities are prohibited:

   a. Acceptance of any terms in research agreements that prevent publication or public presentation of research results or that limit academic freedom without approval.

   b. Acceptance of funding from restricted foreign entities for research with national security implications without prior approval.

   c. Unauthorized sharing of sensitive research data or materials with foreign entities.

   Gifts from a foreign source are managed through UNT Policy 09.002, Fundraising and Private Support. Governmental grants and sponsored projects are managed through UNT Policy 13.007, Sponsored Projects.

5. Cybersecurity Protections

   a. Any individual interacting with CUI must comply with UNT System Regulation

06.10000, Controlled Unclassified Information Protection, to ensure sufficient controls are in place for Controlled Environments.

b. CUI Identification and Management

The Research Security Office shall be responsible for:

i. identifying research data that qualifies as CUI under 32 CFR Part 2002;

ii. ensuring appropriate CUI markings are applied in accordance with the markings as identified by the U.S. National Archives and Records Administration;

iii. establishing handling and storage protocols for CUI;

iv. monitoring compliance with CUI safeguarding requirements; and,

v. coordinating with the UNT System Chief Information Security Officer or delegate on technical implementation of CUI controls.

c. NIST 800-171 Compliance

When federal contracts or grants require protection of CUI:

i. Research systems must comply with NIST Special Publication 800-171.

ii. UNT Academic Technologies shall implement required technical controls.

iii. Principal investigators shall coordinate and complete annual compliance self-assessments with the UNT Research Security Office and the Office of the UNT System Chief Information Security Officer.

iv. The Research Security Office shall verify compliance before CUI collection, creation, analysis, processing and storage.

d. Coordination with Information Security Officer

i. The Office of the Chief Information Security Officer advises and provides oversight on the technical infrastructure for research security controls, encryption, access controls, and monitoring systems.

ii. The Research Security Office and the Office of the Chief Information Security Officer shall jointly respond to incidents involving research data.

iii. Technical disputes shall be elevated to the Chief Information Security Officer for resolution.

e. Cybersecurity Incident Reporting

i. All cybersecurity incidents involving research data must be reported immediately to:

1. The Office of the Chief Information Security Officer; and,

2. The Research Security Office.

6. Conflict of Interest Disclosure and Management

The university has policies and procedures to ensure objectivity in all Research Activities.

Prior to engaging in a Research Activity and annually thereafter, all UNT personnel whose institutional responsibilities include the design, conduct, or reporting of research, either funded or proposed for funding, must complete a research conflict of interest disclosure form and certify that they are not a participant in a Malign Foreign Talent Recruitment Program as defined in UNT Policy 13.005, Conflict of Interest for Sponsored Projects. Changes in status in previously disclosed information must be reported within 30 calendar days of the change.

The Research Security Office reviews all research conflict-of-interest disclosures, including the disclosure of international collaborations, international appointments, and travel sponsored by international entities. When necessary, the Research Security Office will create a conflict-of-interest management plan to provide oversight.

In accordance with NSPM-33 requirements, UNT Policy 13.005, Conflict of Interest for Sponsored Projects, explicitly prohibits participation in malign foreign talent recruitment programs.

In accordance with Texas Executive Order GA 48, UNT prohibits faculty and staff from accepting gifts from FAC, regardless of value, including payment of travel expenses.

Research conflict of interest is managed through UNT Policy 13.005, Conflict of Interest for Sponsored Projects.

As outlined in UNT Policy 04.027, Ethics, UNT employees must also adhere to restrictions regarding acceptance of gifts, secondary employment, and use of institutional resources that may create conflicts of interest or commitment related to foreign influence concerns.

7. Visiting Collaborators Oversight

The University maintains a comprehensive Visiting Collaborators program designed to enhance mutually beneficial Research Activities while safeguarding the interests of the University. All Visiting Collaborators are screened, approved, and managed

through UNT Policy 13.019, Visiting Collaborators. The Research Security Office, working in collaboration with all divisions and units, examines all Visiting Collaborators and provides all UNT employees who play a role in facilitating the collaboration with guidance for hosting visitors to UNT research facilities.

All Research Activities with Visiting Collaborators are subject to a risk assessment conducted by the Research Security Office prior to the initiation of the Research Activity. Risk assessments include, but are not limited to:

a. considerations related to Research Security;

b. export control requirements;

c. conflicts of interest or commitment;

d. intellectual property protections

e. data security and privacy

f. compliance with state and federal regulations; and

g. contributions to UNT's mission.

The Research Security Office conducts supplementary due diligence on potential international Visiting Collaborators including, but not limited to:

a. verification of institutional affiliations;

b. review of publication history and research integrity;

c. identification of funding sources;

d. review of connections to foreign governments or military organizations; and

e. assessments of previous compliance with international agreements.

8. Intellectual Property

The University protects Intellectual Property and critical research data from undue foreign influence. Intellectual Property is controlled by UNT Policy 08.003, Research Intellectual Property.

The Research Security Office will establish procedures to protect Intellectual Property, such as inventions, discoveries, and data, to provide Research Security safeguards around intellectual property to prevent unauthorized disclosure, theft, or exploitation.

Material Transfer Agreements, the protection of Intellectual Property, and commercialization of technology must adhere to UNT Policy 08.003, Research Intellectual Property,

9. Research Risk Assessment and Management

The Research Security Office will perform continuous risk assessments of Research Activities across the UNT research enterprise.

The Research Security risk assessments will identify vulnerabilities, assess potential impact, and develop strategies to mitigate risks effectively. Low-risk collaborations may be approved by the Research Security Officer, medium-risk collaborations must be reviewed by the UNT Research Security Committee, and high-risk collaborations require approval by the Vice President of Research and Innovation and the University Integrity and Compliance Vice President & Chief Integrity Officer.

If, in the determination of the Research Security Officer, any Research Activity under this policy creates a significant Research Security risk, the Research Security Officer may, at the discretion of the Vice President for Research and Innovation, require the Research Security Office to conduct additional due diligence.

The Vice President for Research and Innovation may withhold approval on any Research Activity, under this policy, that could result in any violations or significant risk of any violations of U.S. export control laws or regulations, Research Security laws or regulations, National Security Presidential Memorandum-33 directives, federal research security directives issued by U.S. government agencies, Controlled Unclassified (CUI) safeguarding requirements, federal cybersecurity mandates, Texas Education Code § 51.956 and Texas Executive Order GA 47, Texas Executive Order GA 48, and other applicable state executive orders.

B. Responsible Officials and Responsibilities

1. Research Security Council

In accordance with Texas Education Code § 51.957, UNT shall participate in the Higher Education Research Security Council as a tier one research institution designated as R1 in the 2025 Carnegie Classification.

a. Research Security Council Membership

i. The designated Research Security Officer shall serve as UNT's representative on the Council.

ii. For UNT System Administration, the Chancellor shall designate which Research Security Officer serves as the voting member.

b. Required Research Security Council Activities

The institution shall:

i. Adopt research security policies developed by the Council;

ii. Pursue accreditation for security excellence through the Council's process;

iii. Ensure Research Security Officer participation in the Council's annual training program covering:

1. Background and academic history checks of researchers; and
2. Research security and integrity tools and software;

iv. Participate in Council's best practices development; and,

v. Support the Council's annual academic security and counter exploitation program seminar promotion.

c. Reporting

The institution shall cooperate with the Council's preparation of annual confidential reports to the Governor, Attorney General, and Legislature on research security status.

2. UNT Research Security Committee

The Vice President of Research and Innovation will designate the UNT Research Security Committee and be tasked with reviewing, assessing, and prioritizing potential Research Security risks and making recommendations and the appropriate mitigation strategies to be taken in adherence with federal and state laws and regulations as it relates to the Research Security Program.

3. Research Security Officer

UNT will appoint a Research Security Officer (RSO) in accordance with Texas Education Code § 51.956. The RSO is responsible for:

a. working closely with the UNT Research Security Committee to ensure that investigators and academic units have the relevant information regarding the rapidly changing landscape for international activities and Research Security;

b. conducting initial and ongoing risk assessments for securing sensitive research information and taking action to mitigate institutional risks;

c. developing and implementing procedures for monitoring and incident reporting involving Research Security-related compliance;

d. serving on the Higher Education Research Security Council in accordance with Texas Education Code § 51.957;

e. attending the Academic Security and Counter Exploitation (ASCE) conference at Texas A&M University; and

f. maintaining classified information, maintaining controlled unclassified information, conducting foreign influence reporting, and addressing other issues at the institution associated with the goals of this policy framework.

4. Research Security Point of Contact

   The Research Security Officer shall serve as or designate the Research Security Point of Contact (POC). The Research Security POC shall:

   a. serve as the primary contact for research security inquiries from faculty, staff, students, and external stakeholders;

   b. coordinate with federal research agencies on research security matters;

   c. facilitate research security incident reporting;

   d. provide guidance on research security policy interpretation; and

   e. coordinate with the UNT Research Security Committee on policy development and implementation.

5. Research Security Office

   The Research Security Office is responsible for implementing employment screening and foreign travel preapproval procedures in compliance with Texas Education Code § 51B.152 and Texas Education Code § 51.956. These responsibilities include:

   a. Employment Screening: Reviewing required materials such as citizenship history, curriculum vitae, participation in foreign talent recruitment programs, research funding applications, foreign entity affiliations, foreign institutional appointments, and foreign government-sponsored travel.

   b. Verification and Risk Mitigation: Verifying submitted information and taking appropriate actions to mitigate identified Research Security risks.

   c. Law Enforcement Reporting: Reporting to law enforcement agencies designated by the Governor or UNT's governing board any individuals rejected for employment based on security screening.

   d. International Travel Preapproval: Establishing and implementing a risk-based framework for preapproving employment-related international travel, including criteria, procedures, timelines, and documentation requirements. This process is integrated with UNT's travel policies and Risk Management Services.

   e. Documentation and Coordination: Maintaining written procedures for all screening and approval processes, and coordinating with Human Resources, Academic Affairs, and Risk Management to ensure consistent university-wide implementation.

   f. Additional Responsibilities: Taking reasonable steps to verify information in submissions, taking any other action the office considers appropriate, preapproving certain employment-related international travel according to the established risk-based framework, and maintaining classified information,

Controlled Unclassified Information, conducting foreign influence reporting, and addressing other issues associated with the goals of the Research Security policy framework.

6. University Faculty and Researchers

All UNT employees involved with the research enterprise, including but not limited to, faculty, staff, student researchers, research administrative staff, and visiting collaborators must adhere to the Research Security policies and procedures from the funding agencies and the University to mitigate risks to critical research data and intellectual property and conform to Research Security laws and regulations.

In accordance with UNT Policy 04.027, Ethics, all UNT personnel engaged in Research Activities must maintain the highest standards of ethical behavior and integrity. This includes adherence to all institutional policies including responsible research conduct, disclosure of foreign engagements, and protection of sensitive information. Researchers must ensure that all information provided to the University and funding agencies is thorough and accurate.

In accordance with UNT Policy 04.007, Reporting Suspected Wrongdoing, all UNT employees have the responsibility to make good faith reports of wrongdoing. The University is committed to protecting from retaliation any individual who, in good faith, reports suspected Research Security violations, export control issues, foreign influence concerns, or any reports of wrongdoing.

C. Penalties for Non-Compliance

Failure to comply with this policy and applicable Research Security laws and regulations may result in severe civil and criminal penalties for the University and individuals.

Violations of this policy or other applicable policies may result in restrictions on Research Activities, termination of research projects, withdrawal of funding proposals, return of research funds, or implementation of additional oversight measures.

Any individual who does not comply with the policy may be subject to disciplinary action up to and including termination, dismissal, or expulsion. When required by law or regulation, violations will be reported to appropriate federal or state agencies.

D. Auditing

The UNT Enterprise Office of Internal Audit includes the Research areas within the scope of their risk assessment process. Based on risk and previous reviews, Internal Audit may scope the Research Security program as appropriate, into future Internal Audit reviews.

V. References and Cross-References

15 C.F.R. §791.4
22 CFR § 120.25

E.O. 13292
NIST SP 800-59
NIST Special Publication 800-171
Texas Education Code § 51B.152
Texas Education Code § 51.956
Texas Education Code § 51.957
Texas Executive Order GA 47
Texas Executive Order GA 48
UNT System Regulation 06.10000, Controlled Unclassified Information Protection
UNT Policy 04.007, Reporting Suspected Wrongdoing
UNT Policy 04.027, Ethics
UNT Policy 08.003, Research Intellectual Property
UNT Policy 09.002, Fundraising and Private Support
UNT Policy 09.003, Gift Allocation
UNT Policy 13.005, Conflict of Interest for Sponsored Projects
UNT Policy 13.006, Research Misconduct
UNT Policy 13.007, Sponsored Projects
UNT Policy 13.010, Export Controls
UNT Policy 13.019, Visiting Collaborators
UNT Policy 14.002, Information Security
UNT Policy 15.017, International Travel
National Security Presidential Memorandum-33
U.S. National Archives and Records Administration

VI. Revision History

Policy Contact:	Director, Ethics & International Research Compliance
Approved Date:	2/17/2026
Effective Date:	2/17/2026
Revisions:	