THE UNIVERSITY OF TENNESSEE

System-wide Policy: BT0033 - Policy on Research Security	
Version: 1	Effective Date: 10/25/2024

BOARD OF TRUSTEES
POLICY ON RESEARCH SECURITY

I. PURPOSE

The mission of The University of Tennessee (the "University") is to serve all Tennesseans and beyond through education, discovery and outreach that enables strong economic, social and environmental well-being. Consistent with the Be One UT values, the Board of Trustees (the "Board") is dedicated to governing the University in a manner that will advance the public's trust and confidence in the University and its mission through, among other things: (i) setting high standards; (ii) fostering integrity through openness, accountability, and stewardship; (iii) embracing the free exchange of knowledge and ideas; and (iii) collaborating internally and externally for greater impact.

The Board is committed to safeguarding the University's research enterprise and adhering to federal, state, and all other applicable legal requirements. This policy has been established for the purpose of furthering the highest level of compliance with applicable ethical, legal, regulatory, contractual, and other requirements to secure, protect, and expand the University's research portfolio, including but not limited to the following categories of research: classified, export-controlled, controlled unclassified, and fundamental.

II. SCOPE

This policy applies to the University, including all of its components (i.e., system administration, campuses, and institutes).

III. RESEARCH SECURITY PROGRAM OFFICERS

A. Chief Research Security Officer. The President of the University shall designate a chief research security officer (CRSO) for the University. The CRSO shall be responsible for: (i) ensuring compliance with this Policy and all policies, procedures, and guidelines developed hereunder; (ii) coordinating and overseeing University research security risk assessment and monitoring programs; (iii) advising and coordinating with campus research security officers on research security training, reviews, and program implementation; (iv) referring research security incidents to the appropriate University programs for review and implementing resolution decisions; (v) corresponding with governmental authorities as needed and in coordination with the RSOs and other University personnel; (vi) maintaining a website and other appropriate communication initiatives concerning the University

Research Security Program; and (vii) certifying University compliance with governmental research security program requirements.

B. Campus and Institute Research Security Officers. Each Chancellor shall designate a research security officer (RSO) for their respective campus. The RSO for the University of Tennessee, Knoxville, shall serve as the RSO for the University of Tennessee Institute of Agriculture and the University of Tennessee Space Institute. The Vice President for the Institute of Public Service (IPS) shall designate an RSO for IPS. The RSOs shall be responsible for: (i) implementing their respective campus' research security training, monitoring, risk assessment, reporting, and compliance programs in coordination with appropriate campus offices; (ii) timely reporting research security incidents, program implementation milestones, and changes in campus research security status to the CRSO; (iii) corresponding with governmental authorities as needed and in coordination with the CRSO and other University personnel; (iv) documenting and maintaining campus research security records; and (v) certifying campus compliance with governmental research security program requirements.

IV. UNIVERSITY RESEARCH SECURITY COUNCIL

To promote collaboration and consistency across the University, a systemwide University Research Security Council ("Council") shall be established. The following individuals shall serve ex officio on the Council:

- Associate Vice President for Research*;
- Executive Director of Institutional Compliance*;
- Chief Research Officer of each campus;
- CRSO and each RSO;
- Vice President for National Labs;
- Chief Information Officer for the University;
- Enterprise Risk Officer; and
- Chair, University Faculty Council.

*Co-chairs of the Council.

The University Policy Director, University Director of Privacy, and a member of the Office of General Counsel shall be advisory, non-voting members of the Council.

The University President, Vice President for Academic Affairs, Research and Student Success, the Chief Audit and Compliance Officer, and the General Counsel for the University shall each receive notice of all Council meetings. The Council shall administratively report to the Vice President for Academic Affairs, Research, and Student Success.

V. RESEARCH SECURITY PROGRAM

The Council shall be responsible for evaluating the University's research security posture and for developing an integrated and comprehensive research security program for the University, which shall include administrative policies, procedures, guidance, and training to: (i) ensure the University's compliance with applicable laws, regulations, and other requirements; (ii) provide important resources and tools to assist research active faculty, staff, and students; and (iii) mitigate threats to the integrity and conduct of the University's research enterprise against undue foreign interference (the "Research Security Program").

Such Research Security Program shall address key risk areas identified by federal and state governments, including, but not limited to, intellectual property, cybersecurity, research and proprietary data security, clinical trial data security, disclosure requirements, foreign collaborations, foreign travel security, foreign visitors, foreign scholars and researchers, insider threats, export control, and any other key risk areas identified by the Council or otherwise requested by the President of the University. In developing the Research Security Program, the Council shall implement safeguards to protect the rights of researchers, students, and research support staff and avoid targeting, stigmatization, or unlawful discrimination against individuals.

The Council shall evaluate and report recommendations to the Vice President for Academic Affairs, Research, and Student Success regarding the University offices and positions which are most appropriate to serve as the University's responsible official for subject matter areas included within the Research Security Program.

The Council is authorized to convene working groups comprised of subject matter experts to provide advice to the Council on particular topics and shall seek to integrate the Research Security Program into existing University programs, offices, and departments to maximize efficiency.

A. Council Bylaws. The Council shall adopt bylaws, consistent with this Policy, setting forth the rules and procedures governing how the Council will operate including meeting frequency, voting, committees, special committees, etc. The Council Bylaws shall be maintained on the University System Policy Website.

B. Education and Training. The Research Security Program shall include a training program to ensure that research faculty, staff, and students receive: (i) training required by applicable laws, regulations, and other requirements; and (ii) resources and tools to assist with disclosures, risk mitigation, and ongoing compliance. The training program requirements and objectives shall be developed by the Council and implemented by the CRSO and RSOs in coordination with existing University programs, offices, and departments, as appropriate. The training program shall utilize training resources developed

by governmental authorities when required and shall otherwise leverage governmental resources where appropriate to maximize efficiency.

C. Communication. The Research Security Program shall include communication procedures and processes which facilitate the distribution of governmental and other useful resources, guidance, and communications relevant to the University's research enterprise. At a minimum, the communication procedures and processes shall require the CRSO to create, maintain, and update a University research security website which facilitates access to the Research Security Program materials.

D. Monitoring, Compliance, and Risk Assessment. The Research Security Program shall include systems for research security monitoring, compliance, and risk assessment. The University Office of Audit and Compliance shall conduct periodic compliance reviews of the Research Security Program.

E. Incident Reporting and Response. The Research Security Program shall establish an incident reporting and response program for research security matters. At a minimum, the incident reporting and response program shall require University employees and researchers to report information that may negatively impact the Research Security Program and shall establish a reporting hierarchy, a working group to consider and resolve research security incidents in coordination with necessary University and campus programs and offices, and procedures for resolving research security incidents. 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.

VI. DELEGATED SIGNATURE AUTHORITY

Subject to compliance with applicable Board or University policies requiring prior review of legal instruments by the General Counsel (or designee) and/or the Chief Financial Officer (or designee), the Vice President for Academic Affairs, Research, and Student Success is authorized to execute or cause to be executed such contracts, agreements, certifications, or any other instrument of legal obligation on behalf of the University pertaining to the Research Security Program consistent with the provisions of this Policy and any applicable Board resolutions. This delegation of signature authority is supplemental to, and does not replace, any duly authorized signature authority existing as of the date of this Policy.

Additionally, the Vice President for Academic Affairs, Research, and Student Success may designate in writing, without the right for further sub-delegation, appropriate system, campus, and/or institute administrative personnel the authority to sign certain documents associated with the University's Research Security Program as may be

recommended from time to time by the Council. A copy of the delegation letter(s) shall be filed with the Chief Audit and Compliance Officer, the Chief Financial Officer, and the Board Secretary and Special Counsel.

VII. REPORTS

The Council shall be responsible for preparing an initial implementation report, along with other ongoing reports, pertaining to the University's research program as deemed appropriate by the Audit and Compliance Committee.

History:

Adopted	10/25/2024