The University of Texas at Arlington Research Security Policy Framework

Rationale and Goals

This policy framework is designed to enable UTA to promote secure research while mitigating the risk of foreign influence and intellectual property theft. The provisions listed here, as established by the Education Code Section 51.956, are the guiding principles for promoting an organizational culture of compliance with state and federal requirements (e.g., National Security Presidential Memorandum 33 guidelines). It is the goal of this policy framework to strengthen and protect institutional U.S. government-funded research while fostering an active and international collaborative research environment.

Research Security Officer

UTA is committed to the highest standards of integrity and regulatory compliance in safeguarding its research portfolio. UTA has appointed a research security officer (RSO) as part of the new Texas Legislation. The RSO will report to the Associate Vice President for Research Administration and will be responsible to:

a) Facilitate the implementation of the federal and state requirements related to research security,
b) Ensure that investigators and academic units have the relevant information regarding the rapidly changing landscape for international activities and research security,
c) Conduct initial and ongoing risk assessments for securing sensitive research information and take action to mitigate institutional risks,
d) Develop, implement, and provide oversight of policies, procedures, and associated research security training,
e) Develop and implement procedures for monitoring and incident reporting involving research security-related compliance,
f) Identify and oversee any University employee association to Malign Foreign Talent Programs,
g) Attend academic security and counter exploitation program educational events, including the annual conference at the Texas A&M University, and
h) Advise the Office of the President, Office of the Vice President for Research & Innovation, Office of Information Technology, the Office of Legal Affairs, and the Information Security Office on matters related to research security.

Applicable Policies, Programs, and Processes

To support UTA's ongoing efforts to reinforce and promote research security, policies, programs, and processes will be maintained and enforced in the following areas:

- Research Conflict of Interest and Conflict of Commitment

- Export Control (includes international research collaborations, international travel, vendor assessments, international shipments, and international visiting scholars)
- International Research Travel Oversight (includes travel security)
- Disclosures to Federal Funding Agencies
- Intellectual Property and sensitive research data
- Research Security Plan monitoring for NIST 171 and CMMC Compliance
- Best Research Data Maintenance and Security practices
- UTA's implementation and control environment to comply with NSPM-33 (To be finalized in 2024)

Resources

Foreign Influence on Research

UTA's Export Management and Compliance Program

UTA RA-PO-02 "Policy for Disclosure, Management, and Reporting of Conflicts of Interest in Research"

UTA EI-PO-02 "Conflicts of Interest, Conflicts of Commitment, & Outside Activities Policy"

UTA Cybersecurity Training with KNOWBE4

Responsible Conduct of Research

Research Security Program Framework

I. University Position

Research at UT Austin plays a significant role in advancing a fundamental understanding of the universe, generating creative breakthroughs that lead to technologies with positive benefit, creating opportunities for economic growth in the state, and changing the trajectory of young people through education. Collaboration has long been an important driving force in research. The growth of interdisciplinary approaches and powerful specialized technologies has dramatically elevated the need for and importance of collaborative research. However, the increase of collaborative research, along with differing views of research integrity, has presented some challenges. Protecting intellectual property from undue foreign influence and ensuring research integrity in proposing and conducting research are issues that continue to receive increased attention from Congress and all major federal agencies sponsoring research at UT. Recognizing, understanding, and addressing such challenges and related issues through a comprehensive research security program will help ensure responsible, effective, and productive research collaborations.

The University's research security program is based on the core values of honesty, openness, accountability, objectivity, inclusivity, fairness, and stewardship. All members of the research enterprise have an obligation to uphold these values to promote research integrity, safeguard research technologies appropriately, and foster public trust in research output.

II. Purpose and Objectives

The research security program presents a framework designed to protect the university's research from undue foreign threats by striking a balance between openness and security. The security program has three primary objectives:

a. Foster a culture that focuses on safeguarding the integrity of research and intellectual property while promoting and maintaining an inclusive culture that promotes international engagement and collaborative endeavors;
b. Ensure compliance with U.S., state, and System standards for research security, as well as other ethical, legal, regulatory, contractual, and system standards; and
c. Ensure the University community is well-informed and able to provide ongoing input to the research security program by implementing strategic education and outreach.

III. Program Scope

The research security program implements a risk-based approach to ensuring research data security within the scope of the University's research enterprise. Core components of the program include:

a. research integrity training and insider threat awareness,
b. risk-based monitoring of University research activities,
c. conflict of interest and conflict of commitment disclosure and management,
d. oversight of foreign visitors and collaborators,
e. export compliance,
f. cybersecurity protections, and
g. foreign travel security.

IV. Program Governance

A Research Security Governance Committee is established to provide guidance regarding areas of risk, facilitate inter-campus collaboration, ensure that program components operate effectively within established and evolving University systems, and help facilitate outreach across the institution. Membership includes representatives from Information Security, Legal Affairs, Export Control, Conflict of Interest and Outside Activities, Sponsored Projects, Discovery to Impact, Texas Global, Applied Research Laboratories, Defense Research Advancement, Cockrell School of Engineering, College of Natural Sciences, and Dell Medical School.

V. Responsibilities

A. Research Security Officer

The University establishes a Research Security Officer who will be responsible for ensuring the research security program continues to meet all required federal, state, and System standards and is implemented effectively. The Vice President for Research serves in this role and has delegated authority to the Applied Research Laboratories Research Security Officer for security of classified information and to the Associate Vice President for Research Support & Compliance for security of non-classified and controlled unclassified information.

B. University Faculty and Researchers

All researchers at the University are expected to adhere to research security related policies and procedures of funding agencies and the University to mitigate risks to critical research data and intellectual property. Researchers must ensure that all information provided to the University and funding agencies is thorough and accurate.

THE UNIVERSITY OF TEXAS AT DALLAS
Office of Research and Innovation

Office of the Vice President
800 W Campbell Road AD15
Richardson Texas 75080-3021
T: 972-883-4570 F: 972-883-4569
research.utdallas.edu

Academic Research Security Policy Framework

Research Security and Ethics
Office of Research and Innovation
The University of Texas at Dallas

Section 1. Summary

This framework identifies the values, elements, and responsible persons that comprise the Academic Research Security Program (the Program) for The University of Texas at Dallas (UT Dallas). The Program is intended to ensure UT Dallas complies with State of Texas and US Government requirements for research security, such as the National Security Presidential Memorandum 33 guidelines.

Section 2. Commitment to Compliance and Academic Values

UT Dallas is committed to cultivating and maintaining a secure environment for the performance of federal and industry funded research, protection of intellectual property and research data, and management of other research assets. This commitment requires that UT Dallas provide the infrastructure and personnel to achieve the highest level of compliance with applicable ethical, legal, regulatory, contractual and system standards and requirements in securing research, and to promote an organizational culture of compliance in meeting federal requirements to maintain federal funding.

The operation of the Program will be balanced against the long-held academic values of transparency, integrity, reciprocity, and inclusivity, which are vital to the long-term wellbeing of the UT Dallas academic and research community. The Program will be implemented using a risk-based approach that tailors the security program requirements to the sensitivity of the research activity. A risk-based approach will allow UT Dallas to meet state and federal research security mandates while minimizing the impact on educational and academic activities.

Section 3. Program Mission and Vision

The mission of the Program is to safeguard the research data, intellectual property, funding, facilities, and operations supporting federally funded activities, critical and emerging technology research activities, and other high and moderate impact research activities performed at UT Dallas.

The vision of the Program is to provide policy services, training, operational support, and monitoring to enhance funded research compliance, to safeguard critical and emerging technology research, and to provide support for addressing complex compliance situations and risks.

Section 4. Program Scope

This framework is intended to address the research security risk areas applicable to the UT Dallas research portfolio, including, but not limited to research data security, foreign travel security, foreign relationship oversight, and management of foreign visitors and scholars.

The Program will have administrative responsibility for the following regulatory and policy areas.

1. Critical and emerging technology research safeguards
2. Foreign travel security
3. Foreign funding and relationship reporting
4. Relationships with sanctioned persons and organizations
5. Research data and information classification
6. Research data and information security planning
7. Research risk assessment and management
8. Research visitor access and management

To support institutional compliance with these regulations and to promote a culture of compliance, the Program will undertake the following activities:

1. Lead the development of the necessary policies and procedures to meet government-mandated research security requirements.
2. Provide training and educational opportunities, including regulatory and policy guidance.
3. Provide forums, reports, and other methods for internal communication.
4. Collaborate with partner offices and the Council to develop risk assessment and management tools.
5. Coordinate internal monitoring, noncompliance detection, and incident reporting.
6. Other advice and assistance needed by partner institutional offices in related compliance activities.

Section 5. Responsible Officials and Responsibilities

Academic Research Security Council

The UT Dallas President has designated the Academic Research Security Council (the Council) to oversee the development and implementation of the Program, advise the President concerning the development and implementation of the Program, monitor coordination and collaboration between the institutional offices and stakeholders contributing to the Program, and ensure the development and implementation of the Program is consistent with the institution's academic and research missions.

The Council is comprised of the following UT Dallas executive officers.

1. Vice President and Chief of Staff (Chair)
2. Vice President for Research and Innovation (Vice Chair)
3. Vice President for Academic Affairs and Provost
4. Vice President for Information Technology
5. Vice Provost for Global Engagement
6. Speaker of the Faculty Senate
7. Chief Information Security Officer

Academic Research Security Officer

The UT Dallas President has designated the Academic Research Security Officer (the ARSO) to lead the development and implementation of the Program, ensure the development and implementation of the Program complies with UT System, State of Texas, and federal mandates, facilitate coordination and collaboration between the institutional offices and stakeholders contributing to the Program, and provide administrative support to the Council.

Section 6. Designated Research Units

This framework applies to university research units, and affiliated employees, students and visiting scholars, which meet the qualification criteria set by the Academic Research Security Council. These criteria will reflect the research, technology, and intellectual property priorities of UT Dallas, UT System, the State of Texas, and the US Government. The research units covered by this framework will be determined on a semiannual basis by the Academic Research Security Council. Each designated unit will write and implement a research laboratory security plan under the guidance of the ARSO.

Section 7. Assessment

The UT Dallas Office of Audit and Consulting Services will perform regular assessments of the research security program.

The University of Texas at El Paso

Office of Research
and Sponsored Projects

Research Security

Section:	IV: Research and Sponsored Projects
Chapter:	11
Date Updated:	

11.1 Policy

11.1.1 This policy establishes a framework that promotes secure academic research at the University while mitigating the risk of foreign espionage and interference and ensuring that the institution maintains eligibility for federal funding.

11.1.2 This policy's purpose is to:

11.1.2.1 Achieve compliance with applicable ethical, legal, regulatory, contractual, and system standards and requirements for securing and protecting the institution's research portfolios; and

11.1.2.2 Promote within the institution an organizational culture of compliance with federal requirements.

11.1.3 The University is committed to compliance with applicable federal and state laws and aims to promote a culture of compliance, which includes ensuring that all information provided to the university and funding agencies is thorough and accurate. This policy applies to all faculty, staff, and students, including University research units and affiliated faculty, staff, students, and visiting scholars.

11.1.4 This policy is intended to address the research security risk areas applicable to the University's research, including but not limited to research integrity, cybersecurity protections, research data maintenance, insider threat awareness and identification, foreign travel security, undue foreign influence, oversight of foreign affiliations and funding, oversight of foreign visitors and collaborators, export control, conflict of interest and conflict of commitment disclosure and management, and research risk assessment.

El Paso, Texas
79968-0587
(915) 747-5680
FAX: (915) 747-6474

11.2 Research Security Officer and Implementation of Research Security Compliance Program

11.2.1 A Research Security Officer ("RSO") will be appointed by the President to ensure the implementation of this Policy for purposes of compliance with applicable law and UT System rules and regulations.

11.2.2 The RSO is charged with the responsibility for facilitating compliance with this Policy and development of related procedures and training with the purpose of enhancing awareness of research security risks and measures for mitigating these risks.

11.2.3 The RSO shall work collaboratively with the Provost, appropriate Vice Presidents, Office of Research and Sponsored Projects, Office of Information Security, Office of Institutional Compliance, Office of Legal Affairs, Office of Audit and Consulting Services, UTEP Police Department, the University of Texas System ("U.T. System") Chief Research Security Officer, and the U.T. System Office of General Counsel.

11.3 Noncompliance

Noncompliance with this policy may subject employees to discipline in accordance with applicable University procedures up to and including termination of employment.

11.4 Applicable Policies, Laws, Rules, and Regulations

The applicable policies, laws, rules, and regulations, which are referred to as part of this framework include, but are not limited to:

- National Security Presidential Memorandum - 33 (NSPM-33)
- U.T. System Regents' Rules and Regulations
  - Rule 30101: Conflict of Interest, Conflict of Commitment, and Outside Activities
- U.T. System Policy
  - UTS 165: Information Resources Use and Security Policy
  - UTS 173: Export Controls
  - UTS 175: Disclosure of Significant Financial Interests and Management and Reporting of Financial Conflicts of Interest in Research
  - UTS 180: Conflicts of Interest, Conflicts of Commitment, and Outside Activities
  - UTS 190: International Travel Policy

El Paso, Texas
79968-0587
(915) 747-5680
FAX: (915) 747-6474

- UTEP Handbook of Operating Procedures
  - Section IV: Chapter 2 (Disclosure of Significant Financial Interest and Management and Reporting of Financial Conflict of Interest in Research)
  - Section V: Chapter 29 (Conflicts of Interest, Conflicts of Commitment, and Outside Activities)
  - Section X: Chapter 1 (Information Resources Use and Security Policy)
  - Section X: Chapter 2 (Policy for Compliance with Export Control Regulations)
- All other applicable federal and state laws related to the goals of this policy.

El Paso, Texas
79968-0587
(915) 747-5680
FAX: (915) 747-6474

The University of Texas Permian Basin
Research Security Program Framework

November 17, 2023

Section 1. Summary

This framework identifies the values, elements, and responsible persons that comprise the Academic Research Security Program (the Program) for The University of Texas Permian Basin (UTPB). The Program is intended to ensure UTPB complies with State of Texas and US Government requirements for research security, such as the National Security Presidential Memorandum 33 guidelines.

Section 2. Commitment to Compliance and Academic Values

UTPB is committed to cultivating and maintaining a secure environment for the performance of federal and industry-funded research, protection of intellectual property and research data, and management of other research assets. This commitment requires that UTPB provide the infrastructure and personnel to achieve the highest level of compliance with applicable ethical, legal, regulatory, contractual and system standards and requirements in securing research, and to promote an organizational culture of compliance in meeting federal requirements to maintain federal funding.

The operation of the Program will be balanced against the long-held academic values of transparency, integrity, reciprocity, and inclusivity, which are vital to the long-term wellbeing of the UTPB academic and research community. The Program will be implemented using a risk-based approach that tailors the security program requirements to the sensitivity of the research activity. A risk-based approach will allow UTPB to meet state and federal research security mandates while minimizing the impact on educational and academic activities.

Section 3. Program Purpose and Objectives

The Program presents a framework designed to protect the University's research from undue foreign threats by striking a balance between openness and security. The Program has three primary objectives:

a. Foster a culture that focuses on safeguarding the integrity of research and intellectual property while promoting and maintaining an inclusive culture that promotes international engagement and collaborative endeavors;
b. Ensure compliance with U.S., State, and System standards for research security, as well as other ethical, legal, regulatory, contractual, and system standards; and
c. Ensure the University community is well-informed and able to provide ongoing input to the research security program by implementing strategic education and outreach.

Section 4. Program Scope

This framework is intended to address the research security risk areas applicable to the UTPB research portfolio, including, but not limited to research data security, foreign travel security, foreign relationship oversight, and management of foreign visitors and scholars.

The Program will have administrative responsibility for the following regulatory and policy areas:

1. Critical and emerging technology research safeguards
2. Foreign travel security
3. Foreign funding and relationship reporting
4. Relationships with sanctioned persons and organizations
5. Research data and information classification
6. Research data and information security planning
7. Research risk assessment and management
8. Research visitor access and oversight

To support institutional compliance with these regulations and to promote a culture of compliance, the Program will undertake the following activities:

1. Lead the development of the necessary policies and procedures to meet government-mandated research security requirements.
2. Provide forums, reports, and other methods for internal communication.
3. Collaborate with partner offices to develop risk assessment and management tools.
4. Coordinate internal monitoring, noncompliance detection, and incident reporting.
5. Other advice and assistance needed by partner institutional offices in related compliance activities.

Section 5. Responsibilities

Research Security Officer

The UTPB President has designated the Research Security Officer (RSO) to lead the development and implementation of the Program, to ensure the development and implementation of the Program complies with UT System, State of Texas, and federal mandates.

University Faculty and Researchers

All researchers at UTPB are expected to adhere to research security related policies and procedures of funding agencies and the University to mitigate risks to critical research data and intellectual property. Researchers must ensure that all information provided to the University and funding agencies is thorough and accurate.

The University of Texas Rio Grande Valley
Research Security Program and Framework

Introduction:

Research is a cornerstone in the development of knowledge and innovation. As such, it is critical that research, and the data, innovations, and outcomes it produces, be secured and protected from abuse, theft, or misuse. It is part of The University of Texas Rio Grande Valley's (UTRGV) culture to provide a collaborative approach when enhancing the technology and security across all parts of the institution. This document outlines the basic framework for research security and the **R**esearch **S**ecurity **G**overnance **C**ommittee (RSGC) that oversees research security at UTRGV.

Purpose and Mission:

The purpose and mission of the research security program is to continually improve the safeguards related to research, research data, intellectual property, funding, facilities, and operations supporting both internally and externally funded research activities, especially in the areas of high and moderate impact or critical and emerging technology research, meeting federal, state and UT System rules and regulations. Additionally, a purpose of this program is to ensure that UTRGV maintains the highest standards in regard to compliance with rules, regulations, and laws related to research, including federal, state, UT System, and international regulations that impact research activities.

Program Scope:

The research security program utilizes a risk-based approach to ensure that research, and the data or outcomes produced, adhere to appropriate safeguards across the entire UTRGV enterprise. Core components of this program will be brought together to include but are not limited to:

a. research integrity and insider threat awareness,
b. Intellectual property
c. risk-based monitoring of university research activities,
d. research security risk management and mitigation planning,
e. the classification of research operations and data, including those from clinical studies
f. conflict of interest and conflict of commitment disclosure and management,
g. oversight of foreign visitors and collaborators,
h. export compliance,
i. the development and maintenance of secure research and data storage environments,
j. information and cybersecurity protections,
k. foreign travel security, and
l. training, awareness, and development activities.

Program Governance:

UTRGV's culture is one where groups work across organizational silos to bring skills, expertise, and authorities together to implement institution-wide actions. As such, UTRGV utilizes a governance committee approach that brings operational area expertise into a single collaborative group working to advance research security. The committee will be titled the "**R**esearch **S**ecurity **G**overnance **C**ommittee" (RSGC).

The Research Security Governance Committee consists of:

1. Sr. Vice President for Research (Chair & designated Research Security Official)
2. Exec. Vice President for Finance and Business Affairs and CFO (Co-Chair)
3. UTRGV Chief of Staff
4. Vice President of Human Resources and Talent Development
5. Chief Technology Officer
6. Chair of the International Oversight Committee (International Travel)
7. Chief Information Security Officer
8. Associate Vice President for Research Operations
9. Executive Director Research Compliance and Export Control
10. Associate Vice President of Clinical and Translational Research
11. Chief Audit Officer (Ex officio non-voting member)

The Committee will also ensure that other critical areas of university leadership are included as needed for consultation and communication, such as:

1. Office of the Provost
2. Faculty Senate
3. Office of Institutional Compliance
4. Office of Legal Affairs
5. Office of Student Affairs
6. Procurement Office
7. University Police

Designated Research Security Officer:

UTRGV has designated this committee as the responsible party overseeing the research security program at the institution and to ensure compliance with applicable federal, state and UT System requirements. The chair of the committee will serve as the designated UTRGV Research Security Officer, known at UTRGV as the designated Research Security Official (RSO), to ensure the program and reporting requirements are developed, implanted, and continually improved.

Program Applicability:

This program and its framework apply to all internally and externally conducted University research. This includes employees, , students, consultants, visiting scholars/researchers, and applicable external research persons and entities who meet the criteria established by the Committee. These criteria will reflect the research, technology, and intellectual property priorities of UTRGV, UT System, the State of

Texas, and the US Government. UTRGV will develop and implement a research security risk management plan under the guidance of the Committee, who will review it periodically for consistency with the purpose and mission established.

Research Security Program Framework

I. University Position and Background

There is an increasing need to protect U.S.-funded scientific research from undue foreign influence, including exploitation of the open university research environment and intellectual property theft. The Framework is intended to ensure UTSA complies with the State of Texas and US Government regulations regarding research security, such as the National Security Presidential Memorandum 33 guidelines.

The Research Security Program Framework details the activities, policies, and responsibilities to be compliant with federal and state regulations to promote and protect secure academic research at the institution while mitigating the risk of foreign espionage and interference by providing policies, services, training, operational support, and monitoring to enhance research compliance, to safeguard critical and emerging technology research, and to provide support for addressing complex compliance situations and risks.

NSPM-33 requires a certification from research organizations awarded more than $50 million per year in total Federal research funding, that they have implemented a research security program that includes the four elements:

- Cybersecurity
- Foreign travel security
- Research security training
- Export control training

II. Applicable Policies

University policies are accessible through a central Policy website. Individual policies and procedures are reviewed and updated as needed with the latest revision noted below each policy heading.

- Conflicts of Interests and Conflicts of Commitment: HOP 10.04 Conflicts of Interest in Research & Intellectual Property
- Research Misconduct: 10.02 Misconduct in Research or in Other Scholarly Activities
- Export Control: HOP 10.01 Export Controls
- Data Access, Management, and Transfer: HOP 10.09 Research and Other Sponsored Projects Data or Record Ownership and Retention
- Cybersecurity: HOP 11.04 Information Security Incident Response

Disclosure Requirements

Workflows and processes have been revised to prompt disclosures from new hires, contractors, and international visiting scholars during the onboarding process with an emphasis on the importance of disclosing foreign contracts, affiliations, and disclosing involvement with foreign talent recruitment programs. Foreign affiliation disclosures are routed to the Research Security Manager in the ORII for export control and research security risk assessment and may involve a management plan as a condition for collaboration. The use of loaner devices is currently being managed at the college level.

Violation of disclosure requirements may have criminal., civil, and/or administrative consequences. UTSA investigators are ultimately responsible for ensuring that they make all appropriate disclosures required by sponsors and internal policy and follow any prescribed plan for the management, reduction, or elimination of a real or perceived risk identified in a disclosure. Failure to do so is a violation of University Policy. The investigator's department, Dean, and/or the Conflict-of-Interest Office may inspect records to ensure compliance with the plan. Failure to report a significant financial interest or failure to cooperate in a conflict-of-interest management plan may be cause for disciplinary action up to and including dismissal. Possible violations of policy include, but are not limited to providing false, misleading, or incomplete information.

III. Scope and Responsibilities

Cybersecurity

a. Provide regular cybersecurity awareness training for authorized users of information systems, including in recognizing and responding to social engineering threats and cyber breaches. Awareness training is covered in a module in annual institution-wide compliance training.
b. Limit information system access to only authorized users, processes acting on behalf of authorized users, or devices (including other information systems). The Office of People Excellence coordinates authorization through procedures for employees and Persons of Interest.
c. Limit information system access to the types of transactions and functions that authorized users are permitted to execute. Access is controlled. The Office of Institutional Compliance and Risk Services and the Office of Internal Audit verify these controls.
d. Verify and control/limit connections to and use of external information systems. The Office of University Technology Services has implemented next-generation firewall and perimeter protections and the Office of Information Security conducts annual security risk assessments with external systems to verify security controls have been effectively implemented.
e. Control any non-public information posted or processed on publicly accessible information systems. UTSA utilizes Category I, II, II data use rules to control data published on systems. Identify information system users, processes acting on behalf of users, or devices. UTSA promotes the use of service accounts where needed and monitors user behaviors on east-west traffic through network detection and response solution that has been implemented.
f. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational information systems. UTSA requires modern authentication to central systems and utilizes MFA where applicable.
g. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. UTSA maintains NGF firewalls with policies that explicitly control connections to the edge network. Internal segmentation exists based on use-cases and requirements.
h. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. UTSA utilizes zones within our network for publicly accessible services that are separate from internal networks.
i. Provide protection of scientific data from ransomware and other data integrity attack mechanisms. UTSA utilizes anti-malware and in-line vision infrastructure monitoring.
j. Identify, report, and correct information and information system flaws in a timely manner. Weekly vulnerability scan results are analyzed and processed according to criticality.
k. Provide protection from malicious code at appropriate locations within organizational information systems. UTSA utilizes Microsoft Defender and Malware Bytes for endpoint protection from malware.
l. Update malicious code protection mechanisms when new releases are available. UTSA updates antimalware as a matter of course and adheres to strict change management practices.
m. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. UTS performs weekly scans using Nessus and Tenable.

CUI (Controlled Unclassified Information - when applicable)

a. The Research Security Manager (RSM) plays a crucial role in providing guidance to faculty and working collaboratively with RSC and contract negotiator staff throughout the award/contract process. It is imperative that input from the CISO is taken into consideration during these negotiations to ensure the utmost security measures are implemented.

b. UTSA's Research Computing group should provide guidance for secure computing capabilities and appropriate storage locations. This guidance should include procedures, training, and delegation of responsibilities specifically related to CUI.

Foreign Travel Security

Maintain international travel policies for faculty and staff for business travel that would put a person at risk. The below measures have been implemented:

a. **Prior disclosure and approval requirement**: The UTSA Request for Travel Authorization includes a flag if the travel is outside the U.S. to a location identified as "Restricted" by the US federal government, which automatically notifies the Research Security Manager (RSM).

b. **Security briefings:** The RSM performs a security briefing process for all research personnel traveling internationally.

c. **Electronic device assistance:** UTSA Libraries has loaner laptops available for students. Departments and Colleges have spare laptops available for faculty and other research personnel.

Research Security Training

Relevant personnel receive training such as research security threat awareness and identification and insider threats. These topics should also be incorporated into the responsible conduct of research training. Specialized training should occur in the event of a research security incident. The RSM provides briefings on an as-needed basis. The program could be expanded from only those working with controlled technologies to those researchers who work in areas identified as high-risk for security threats.

Export Control Training

Export control training (when appropriate) is provided to relevant personnel when research is subject to export control restrictions per the sponsored project award document. The RSM provides briefings to all research personnel working with research subject to export controls. These briefings are included as a requirement of Technology Control Plans. Export Control training is also offered to administrative and other support staff as well. The training includes requirements and processes for reviewing foreign sponsors, collaborators, and partnerships, and for ensuring compliance with federal export control requirements and restricted entities lists.

IV. Responsibilities

Research Security Officer

The University establishes a Research Security Officer who will be responsible for ensuring the research security program continues to meet all required federal, state, and System standards and is implemented effectively. The Vice President for Research serves in this role and has delegated authority to the Research Security Manager of classified information and controlled unclassified information.

University Faculty and Researchers

All researchers at the University are expected to adhere to research security related policies and procedures of funding agencies and the University to mitigate risks to critical research data and intellectual property. Researchers must ensure that all information provided to the University and funding agencies is thorough and accurate.

IV. Designation and Accessibility of a Research Security Point of Contact

The Associate Vice President, Research Integrity and Infrastructure in the Office of Research, Economic Development, and Knowledge Enterprise is the institution's point of contact.

Research Security Framework
Stephen F. Austin State University
Office of Research and Graduate Studies

The SFA Office of Research and Graduate Studies mission is to inspire and empower our students and faculty to achieve excellence in advanced learning, innovation, discovery, and/or creative activity.

In support of our mission, we commit to the development and implementation of the Research Security Framework and by doing this ORGS will address these research security risks identified by SFASU through the following activities:

- Ensure researchers are compliant with Federal, State, System, and Sponsor regulations,
- Ensure we are clearly communicating values, standards and integrity as a university,
- Provide ongoing trainings for all employees to educate them about the risks and their responsibilities,
- Encourage employees to report any suspicious activities.

Pursuant to Texas Education Code 51.956 this policy aims to protect SFA's research that is funded from government entities. SFA has appointed a Research Security Officer as part of this new Texas Legislation. National Security Presidential Memorandum, (NSPM-33)- requires institutions to have certain controls in place for ensuring our institution is providing the required trainings and implementing appropriate safeguards to protect SFA's funded research.

To support institutional compliance with these regulations and to promote research security, the following additional activities will be implemented:

- Provide export control, research security, insider threat, and cyber security training,
- Review conflict of interest and conflict of commitment disclosure related to research,
- Coordinate with the International Oversight Committee,
- Develop and implement procedures for monitoring research associated with high-risk research projects,
- Ensure faculty and researchers are compliant with Federal, State, System and Sponsor regulations, and

- Ensure faculty and researchers have relevant information regarding the rapidly changing landscape for international activities and research security.

The designated Research Security Officer will oversee the development and implementation of the new research security program which includes, but is not limited to the following responsibilities:

- Work with SFA faculty and staff in implementing a research security program,
- Attend the annual academic security conference at Texas A&M University,
- Coordinate with the International Research Travel Oversight Committee,
- Coordinate with the President's Office, Provost Office, Dean of Research and Graduate Studies, Office of Information Technology Services, and Office of General Council.

UT Tyler
THE UNIVERSITY OF TEXAS AT TYLER

November 20, 2023

Research Security Program Framework

Rationale

This policy framework identifies the elements, and responsible persons involved in the Research Security Program for The University of Texas at Tyler (UT Tyler) and is intended to enable UT Tyler to promote secure research while mitigating the risk of foreign influence and intellectual property theft. The provisions of the Research Security Program are established to promote organizational culture of compliance with State of Texas and US Government such as the National Security Presidential Memorandum 33 guidelines. The overreaching goal is to strengthen and protect institutional research while fostering an active and international collaborative environment.

Objectives

UT Tyler will continue maintaining a secure environment for the conduct of research and the management of research assets, including protection of intellectual property and research data. UT Tyler provides the necessary infrastructure and personnel to uphold compliance with all applicable ethical, legal, regulatory, contractual and system requirements in securing research, and to promote an organizational culture of compliance.

The research security program presents a framework designed to protect UT Tyler's research from undue foreign threats by striking a balance between openness and security. The research security program has three primary objectives that comprise: 1. fostering a philosophy that focuses on safeguarding the integrity of research and intellectual property while promoting and maintaining an inclusive culture that stimulates international engagement and collaborative endeavors; 2. compliance with U.S., state, and System standards for research security, as well as other ethical, legal, regulatory, contractual, and system standards; and 3. ensuring that the University community is well-informed and able to provide ongoing input to the research security program by implementing strategic education and outreach.

Program Scope

The research security risk areas include, but are not limited to research data security, foreign travel security, foreign relationship oversight, and management of foreign visitors and scholars.

The research security program implements a risk-based approach to ensuring research data security within the scope of the University's research enterprise. Core components of the program include:

1. Conflict of Interest and Conflict of Commitment
2. Export Control (includes international research collaborations, international travel, vendor assessments, international shipments, and international visiting scholars)
3. International Travel Oversight (includes travel security)
4. Disclosures to Federal Funding Agencies
5. Intellectual Property Disclosure and Safeguards
6. Cybersecurity
7. Research Data Maintenance

Program Oversight

A Research Security Advisory Committee (RSAC) will be established by the Research Security Officer to provide guidance regarding areas of risk, facilitate inter-campus collaboration, ensure that program components operate effectively, and help facilitate outreach across the institution. Membership includes representatives from Information Security, Sponsored Programs Administration, Institutional Compliance, Human Research Protections Program, and Research Integrity.

The RSAC will be responsible for:

- Advising the RSO on matters related to research security.

- Environmental scanning of ongoing federal funding agency research security requirements and guidance.
- Reviewing current and ongoing efforts for effectiveness.
- Conducting risk assessments.
- Reviewing and recommending training opportunities.
- Coordinating internal monitoring and reporting incidents to the RSO, who will in turn report relevant incidents to the UT System Chief Research Security Officer (CRSO).

Research Security Officer

The UT Tyler appointed a research security officer (RSO) as part of the new Texas Legislation who will be responsible for ensuring the research security program continues to meet all required federal, state, and System standards and is implemented effectively. The RSO will:

a) Facilitate the implementation of the federal and state requirements related to research security,
b) Work closely with the RSAC to ensure that investigators have the relevant information regarding the rapidly changing landscape for international activities and research security,
c) Conduct early risk assessments and take action to mitigate institutional risks,
d) Develop, implement, and provide oversight of policies, procedures, and associated research security training, and,
e) Attend the annual academic security and counter exploitation program educational events, including the annual conference at Texas A&M University.

University Faculty and Researchers

All researchers at the University are expected to adhere to research security related policies and procedures of funding agencies and the University to mitigate risks to critical research data and intellectual property. Researchers must ensure that all information provided to the University and funding agencies is thorough and accurate.

UT Southwestern Medical Center Research Security Policy Framework

Final – 11.30.23

Rationale and Goals

This policy framework is designed to enable UT Southwestern to promote secure research while mitigating the risk of foreign influence and intellectual property theft. In compliance with Tex. Educ. Code § 51.956, this policy framework provides the guiding principles for promoting an organizational culture of compliance with state and federal requirements (e.g., National Security Presidential Memorandum 33 guidelines). It is the goal of this policy framework to strengthen and protect institutional U.S. government-funded research while fostering an active and international collaborative research environment.

Research Security Officer and Research Security Steering Committee

UT Southwestern is committed to the highest standards of ethical, legal, regulatory, contractual and system standards and requirements in safeguarding its research portfolio. On August 30, 2023, UT Southwestern appointed a research security officer (RSO), prior to September 1, 2023 when § 51.956 became effective. The RSO, with support from the Office of Research Support and Regulatory Management, has established a Research Security Steering Committee (RSSC) that will:

a) Facilitate the implementation of the federal and state requirements related to research security,
b) Work closely with the RSO to ensure that investigators and academic units have the relevant information regarding the rapidly changing landscape for international activities and research security,
c) Conduct early risk assessments and take action to mitigate institutional risks,
d) Develop, implement, and provide oversight of policies, procedures, and associated research security training, and
e) Attend the educational and training events, including the Academic Security and Counter Exploitation Seminar hosted annually by Texas A&M University.

Members of the RSSC include representatives from the following UTSW offices and business units:

- Office of Legal Affairs

- Information Security
- Sponsored Programs Administration
- Research Support and Regulatory Management (Conflict of Interest, Conflict of Commitment, and Export Control)
- Office of Institutional Compliance and Audit Services
- Office of Technology Development
- Information Resources - Research and Academic Services
- Human Research Protections Program
- Ethics and Responsible Conduct of Research
- Research Integrity
- Faculty

The RSSC will be responsible for:

- Advising the RSO, President, Provost, and Vice Provosts on matters related to research security
- Monitoring ongoing federal funding agency research security requirements and guidance
- Reviewing current and ongoing efforts for effectiveness
- Conducting risk assessments
- Reviewing and recommending training opportunities
- Coordinating internal monitoring and reporting incidents to the RSO, who will in turn report relevant incidents to the UT System Chief Research Security Officer (CRSO)

Applicable Policies, Programs, and Processes

To support UT Southwestern's ongoing efforts to support and promote research security, committees, policies, programs, and processes will be maintained and enforced in the following areas:

- Conflict of Interest and Conflict of Commitment
- Export Control (includes international research collaborations, international travel, vendor assessments, international shipments, and international visiting scholars)
- International Travel Oversight (includes travel security)
- Disclosures to Federal Funding Agencies
- Intellectual Property Disclosure and Safeguards
- Cybersecurity

- Research Data Maintenance
- Clinical Trial and Patient Safety

Contact Information

The UT Southwestern Research Security Officer can be contacted at ResearchSecurity@UTSouthwestern.edu.

Pending – Web page on EDU site

utmb Health

UTMB Health Research Security Policy Framework

Rationale and Goals

This policy framework identifies the values, elements, and responsible persons that comprise the Research Security Program (the Program) for The University of Texas Medical Branch (UTMB). The Program is intended to ensure UTMB's compliance with US and State of Texas Government requirements for research security, such as the National Security Presidential Memorandum 33 guidelines (NSPM-33). This policy serves to support UTMB's endeavor and commitment to ensuring research security by mitigating the risks of foreign influence and intellectual property theft while encouraging constructive international research collaboration.

NSPM-33 requires covered research organizations to designate a research security point of contact and manage the required elements as an integrated program. Covered research organizations must maintain clear response procedures to address reported allegations of research security non-compliance. They also must report incidents of research security violations to federal awarding agencies.

Research Security Officer and Research Security Council

UTMB is committed to maintaining a research security program that promotes the highest standards of integrity and regulatory compliance. UTMB has appointed a Research Security Officer (RSO). The RSO chairs the Research Security Council (RSC), which is responsible for:

a) Establishing and maintaining international travel policies for covered individuals engaged in federally funded R&D who are traveling internationally for organizational business, teaching, conference attendance, research purposes, or who receive offers of sponsored travel for research or professional purposes.
b) Requiring research security training to be regularly updated and include components such as research security and insider threat awareness and identification.
c) Providing oversight of cybersecurity measures and the baseline safeguarding protocols and procedures for information systems used to store, transmit, and conduct federally funded R&D.
d) Requiring training related to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators, and partnerships and for ensuring compliance with federal export control requirements and restricted entities lists.

Members of the RSC include representatives from the following areas at UTMB:

- Office of Institutional Compliance
- Office of Technology Transfer
- Office of Information Security
- Office of Enrollment Services
- Research Administration Office
- Office of Research Regulations and Compliance
- Faculty

Applicable Policies, Programs, and Processes

To support UTMB's ongoing efforts to promote research security policies, programs, and processes will be maintained and enforced in the following areas:

- Conflict of Interest and Conflict of Commitment
- Export Control (includes international research collaborations, international travel, vendor assessments, international shipments, and international visiting scholars)
- International Travel Oversight (includes travel security)
- Sponsored Programs
- Disclosures to Federal Funding Agencies
- Subrecipient Monitoring
- Intellectual Property Disclosure and Safeguards
- Cybersecurity
- Research Data Maintenance
- Clinical Trial and Patient Safety

Research Security Framework

Policy Number: TBD

Subject: Research Security Framework to ensure research integrity and protect the research enterprise against the misappropriation of research and foreign government interference.

Scope: Members of the University community who are involved in the research enterprise.

Date Reviewed: December 2023

Responsible Office: Office of the Senior Vice President for Academic and Faculty Affairs

Responsible Executive: Senior Vice President for Academic and Faculty Affairs

I. POLICY AND GENERAL STATEMENT

The University of Texas Health Science Center at Houston ("University") strives to create a research climate that promotes integrity in research and fosters innovation. Use of advanced specialized technologies and interdisciplinary approaches have significantly amplified the need for and significance of collaborative research. Increase in collaborative research has presented challenges in ensuring research integrity in the conception and execution of research projects and in safeguarding research from unwarranted foreign influence.

Recognizing, comprehending, and addressing these challenges and related matters through the implementation of a comprehensive research security program is crucial to ensure responsible, efficient, and productive research collaborations. The University's research security program is firmly grounded in core values such as honesty, transparency, accountability, objectivity, inclusivity, fairness, and stewardship. The research security program is intended to ensure that the University complies with State of Texas and US Government requirements for research security, such as the National Security Presidential Memorandum 33 guidelines and Texas Education Code Sec. 51.956. The research security program is intended to ensure that the University complies with applicable federal and state laws and regulations and University of Texas System (U.T. System) requirements. All participants in the research enterprise bear the responsibility of upholding these values to

promote research integrity, properly protect research technologies, and cultivate public trust in the outcomes of our research endeavors.

II. DEFINITIONS

Research Security: 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.

Secure Collaborative Research: Collaboration that ensures secure channels for data and communication, and includes using administrative, technical, and physical security safeguards such as encrypted communication, secure file sharing platforms, and guidelines for any research that is coordinated between or among researchers, institutions, organizations, and/or communities.

III. PROCEDURE

This policy provides an overview of the University's research security framework and links to other policies implementing portions of that framework. The overall aim is to create a secure and responsible research environment that upholds the integrity of scientific and scholarly work while addressing security challenges.

A. Core Components of the Research Security Program

1. Conflict of interest and conflict of commitment disclosure and management: The University has robust procedures and workflows to solicit and review disclosures from faculty and staff and new hires including questions about foreign contracts, affiliations, and involvement with foreign talent recruitment programs. (HOOP 20, HOOP 94, HOOP 221.)
2. Cybersecurity protections: The University has policies and procedures, including data encryption, access controls, and secure storage practices, designed to protect research data, including sensitive and confidential information, from unauthorized access, loss, or breach. (HOOP 175, HOOP 180).
3. Disclosures to federal funding agencies: The University has policies and procedures governing the research enterprise, including requirements that all current and pending "other support" be disclosed in federal grant applications.(HOOP 64, HOOP 93, HOOP 168)
4. Export compliance: The University has policies and procedures to promote compliance with relevant laws, regulations, and funding agency guidelines. This includes export control regulations and other legal requirements related to research activities. (UTS 173 and HOOP *[to come]*)
5. Foreign travel security: The University has policies and procedures to promote 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 to minimize risks of foreign interference and intellectual property theft. (UTS 190, UTS 173, International Travel Mandates).

6. Oversight of foreign visitors and collaborators: The University maintains a robust Visiting Scholars Program to help structure associations with visiting scholars and to protect the interests of the University and the Visiting Scholars. (HOOP 125)
7. Protecting intellectual property: The University has policies and procedures designed to safeguard valuable research findings, technologies, and intellectual property against theft, unauthorized access, and foreign influence in order to preserve the rights and interests of the researchers and their institutions. (HOOP 201, HOOP 180)
8. Research security training and insider threat awareness: The University provides training and awareness programs 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. (HOOP 95)
9. Research integrity: The University strives to create a research climate that promotes faithful adherence to high ethical standards in the conduct of research. (HOOP 202)
10. Auditing and risk-based monitoring of university research activities: The University has a risk management framework including audit, assessment, control, communication, and monitoring including risk assessments to identify vulnerabilities in research projects, assess their potential impact, and develop strategies to mitigate risks effectively.(HOOP 66)

B. Program Governance

The University has established a Research Security Officer (RSO) who will be responsible for ensuring that the research security program continues to meet all required federal, state, and UT System standards as described in more detail below. The Senior Vice President for Academic and Faculty Affairs serves in this role.

A Research Security Workgroup has been established, which may include representatives from the following areas:

1. Conflict of Interest Program
2. Information Technology Security
3. Sponsored Projects Administration
4. Legal Affairs
5. Visiting Scholar Program
6. Technology Management
7. Institutional Compliance
8. Research Compliance
9. Safety, Health, Environment and Risk Management
10. Graduate education and mentorship
11. Faculty
12. UT Police Houston

C. Responsibilities

Research Security Officer
The RSO will be responsible for:
1. Overseeing policies, procedures, and research security training programs designed to promote compliance with federal and state regulations and UT System policies pertaining to research security.
2. Providing researchers with up-to-date information on the dynamic international landscape and research security.
3. Assessing risks and taking measures to mitigate institutional vulnerabilities.

Research Security Workgroup
The Research Security Workgroup will be responsible for:
1. Providing guidance to the RSO on research security issues.
2. Continuously monitoring applicable laws, regulations, and federal funding agency research security requirements and guidance and ensuring University policies are in compliance with these requirements.
3. Evaluating the effectiveness of existing initiatives and proposing changes when necessary.
4. Providing information about research security training options for the research community.
5. Managing internal monitoring and reporting incidents to the RSO, who will report these incidents to the UT System Chief Research Security Officer (CRSO) as required.

University Faculty and Researchers
All researchers at the University are expected to adhere to research security related policies and procedures of funding agencies and the University to mitigate risks to critical research data and intellectual property. Researchers must ensure that all information provided to the University and funding agencies is thorough and accurate.

Research Security incidents will be managed according to the relevant HOOP policy.

IV. CONTACTS

Contact	Telephone	Email/Web Address
Office of the Senior Vice President for Academic and Faculty Affairs	*[to come]*	research@uth.tmc.edu

7.10.n Research Security Program

Chapter 7 - Research and Sponsored Programs	Original Effective Date: Click or tap to enter a date.
Section: 7.10 Research Administration	Date Last Reviewed: November 2023
Responsible Entity: Vice President for Resarch	Date Last Revised: November 2023

I. Purpose

The purpose of this policy is to define the scope, function, and composition of the Research Security Program ("Program") to safeguard UT Health San Antonio's research portfolio and intellectual property against internal and external threats and to ensure compliance with U.S., State of Texas, and UT System requirements. The Program has three primary objectives:

A. Establish shared governance that focuses on promoting research integrity and safeguarding intellectual property by utilizing a risk-based approach when assessing international engagement and collaborative endeavors;

B. Ensure institutional compliance with U.S., state, and System ethical, legal, regulatory, contractual, and standards for research security, including, but not limited to, Education Code Section 51.956 and National Security Presidential Memorandum 33; and

C. Promote a culture of compliance by implementing strategic education and outreach.

II. Scope

The Program addresses risk related to UT Health San Antonio's research portfolio, including, but not limited to research data security, foreign travel, foreign collaborations, and management of foreign visitors and scholars.

The Program will provide governance for the following regulatory and policy subjects:
1. Critical and emerging technology research safeguards
2. Technology and data security for foreign travel
3. Foreign funding and reporting

4. Relationships with U.S. sanctioned persons and organizations
5. Research data classification
6. Research data information security planning
7. Research risk assessment and management
8. Research visitor access and management
9. Information security training and awareness programs associated with research data use and access

III. Policy

A. Governance

UT Health San Antonio's President shall designate a Research Security Center of Excellence to provide diverse stakeholder engagement in the development, implementation, and sustainment of the Program, advise the President and institutional leadership on research security concerns, and ensure the Program is consistent with the institution's research missions.

B. Responsibilities

The Research Security Center of Excellence shall:

1. Support compliance with legal, regulatory, contractual, and standards for research security, including, but not limited to, Education Code Section 51.956 and National Security Presidential Memorandum 33:
2. Lead the development of necessarily policies, standards, and procedures to meet compliance with U.S., state, and System research security requirements;
3. Provide training and educational opportunities, including regulatory and policy guidance, risk reduction practices, and cybersecurity awareness.
4. Develop risk assessment and management tools
5. Coordinate internal monitoring, noncompliance detection, and incident reporting
6. Other guidance and assistance needed by research administration and support offices

C. Membership

The Center of Excellence shall include representatives from:
1. Information Security
2. Office of Sponsored Programs
3. Research Compliance Office
4. Institutional Compliance & Privacy Office
5. Research Protections Programs

6. Faculty
7. Office of Technology & Commercialization
8. Legal Affairs

UT Health San Antonio's President shall designate a Research Security Officer who will be responsible for ensuring the research security program continues to meet all required federal, state, and System standards and is implemented effectively.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

Texas Education Code Section 51.956

National Security Presidential Memorandum 33

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

D. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

E.

Effective Date	Action Taken	Approved By	Date Approved

THE UNIVERSITY OF TEXAS
MD Anderson Cancer Center
Making Cancer History®

FY24 Research Security Policy Framework

Institutional Compliance | December 4, 2023

Purpose and Objectives

The purpose of MD Anderson's Research Security Policy Framework (Framework) is to:

- achieve the highest level of compliance with applicable ethical, legal, regulatory contractual, and system standards and requirements for securing and protecting MD Anderson's research portfolios;
- promote within MD Anderson an organizational culture of compliance with federal requirements to ensure the institution maintains eligibility for federal funding; and
- designate a person to serve as a Research Security Officer (RSO), responsible for maintaining classified information, maintaining controlled unclassified information, conducting foreign influence reporting, and addressing other issues at MD Anderson associated with the goals of the Framework.

The Framework (Current State)*

At present, MD Anderson's Framework is a matrixed structure of programmatic resources that provides strategic direction and guidance on issues related to research security, including but not limited to international collaboration (including international travel); proper disclosure of foreign support on research awards; and risk mitigation of undue foreign influence on research (see Fig. 1, below). However, MD Anderson anticipates significant changes to its Framework with the future installation of a stand-alone RSO. The initiative to build a best-in-breed RSO and resultant Framework are under way and likely will extend beyond the February 21 -22, 2024, Board of Regents' Meeting. Therefore, MD Anderson respectfully requests an extension of the deadline to file its final Framework.

1.0 Operations

Daily operations in the Framework are carried out by a number of teams with interlocking functions and complimentary expertise. **Institutional Compliance** (**IC**) works closely with MD Anderson's **Office of Sponsored Programs** (**OSP**), the central office for administration of all aspects of grant proposal review, regarding matters concerning disclosures to federal and state granting authorities regarding Other Support, Foreign Component, and completeness of Principal Investigator Biosketches. **Institutional Compliance** works with **Travel and Finance** to ensure compliance with NSPM-33/OSTP Guidance on Research Security elements and to incorporate those elements into the institution's international travel program. **Cybersecurity** and **Institutional Compliance** partner to mitigate undue foreign influence risk factors, including reviews and investigations of potential IP data misappropriation.

Established in 2020, the **Office of International Collaboration** (**OOIC**) is a storefront operation run by **Institutional Compliance** that serves as the primary resource to our faculty and researchers for guidance on meeting federal requirements when engaged in "Substantive External Collaboration," defined by MD Anderson policy to include "any work or projects to be performed by Covered Individuals, with any non-

* MD Anderson's Executive Leadership has directed the Senior Vice President and Chief Regulatory Officer and the Chief Compliance & Ethics Officer to prepare a set of recommendations for a stand-alone, independent, dedicated RSO, with independence and a clear scope of responsibility and authority based on best practices culled from both industry and academia. Accordingly, the future state of MD Anderson's Research Security Policy Framework is likely to differ significantly.

United States entity, regardless of compensation, and where programmatic involvement or the use of The University of Texas or MD Anderson resources is anticipated." Working with the **OSP**, the **OOIC** also reviews faculty and researcher COI disclosures for proper compliance with National Institutes of Health "Other Support" and "Foreign Component" disclosure requirements and hosts resources explaining the risks of undue foreign influence and foreign talent recruitment programs.

Further, the **OOIC** provides the administrative support for the **International Collaboration Council** (**ICC**), a multidisciplinary, executive-level committee that provides strategic direction to the institution on matters including international travel and Principal Investigator and institution-level collaborations. Per its charter, the purpose of the **ICC** is to "facilitate international collaborations in a manner that furthers MD Anderson's mission and complies with applicable law." In advancing its purpose, the **ICC** is responsible for informing workforce members with proposed international travel of available MD Anderson and UT System resources; reviewing international collaborations for appropriate use, allocation, and stewardship of resources; ensuring compliance with federal and state law; and performing other duties as assigned by the President. Reporting to the **ICC** is Travel and Finance's **Travel Oversight Committee** (**TOC**), which ensures that travel to international destinations is compliant with NSPM-33/OSTP Guidance on Research Security, including the requirement that research security training be conducted prior to travel.

2.0 Governance

Several committees and offices provide governance over these operations. Formally established on March 16, 2023, the **Science, Technology, and Research Compliance Committee** (**STARCC**) is organized within MD Anderson's compliance committee structure as a subcommittee of both the **Executive Research Compliance Committee** (**ERCC**) and the **Information Security Compliance Committee** (**ISCC**). The **STARCC** was created to promote the security of information resources and other products resulting from research efforts led or supported by MD Anderson. Part of the committee's charge is to monitor and identify information and physical security gaps, identify emerging risks in research security, and develop recommendations to strengthen our research security processes. The committee is co-chaired by MD Anderson's Vice President of Research Strategy and Operations and our Vice President of Academic Affairs, and the voting membership is composed primarily of MD Anderson faculty members, with several relevant administrative subject matter experts serving in *ex officio* roles. Moreover, as this committee includes our Chief Information Security Officer as a permanent committee member and reports up to the ISCC, many cybersecurity issues also will be addressed through this committee.

The **STRCC**, **ISCC**, and **ERCC** all report to the **Executive Institutional Compliance Committee** (**EICC**), which comprises the President, the **Chief Scientific Officer** (**CSO**), the **Chief Academic Officer** (**CAO**), and members of the Division of Legal and Regulatory Affairs. The **EICC** has jurisdiction to review and approve or alter all research security initiatives covered by the other governance committees and serves as the final decision-making and strategy-setting body.

Currently, the Chief Compliance and Ethics Officer serves as MD Anderson's RSO in an interim capacity, pending realization of MD Anderson's goal of enhancing its framework to a best-in-breed Framework.

Fig. 1. MD Anderson's RSO Framework (State as of December 2023)