DIVISION OF RESEARCH & INNOVATION
Research Integrity & Compliance

Visiting Scholar Processes and Procedures

UNT faculty and researchers must complete the following screening processes before initiating a research collaboration, visiting scholar arrangement, industrial affiliate relationship, or other institutional research relationship, including unrestricted gifts supporting research, with an entity that has been determined to present elevated risks for export control or information security "Sensitive Entity".

The Division of Research, Division of International Affairs, and the Information Security Office will assist faculty in identifying Sensitive Entities proposing a relationship with the university. The determination of risk will be based on information provided to UNT by a federal or state agency and/or information in the public domain, including the individuals and entities identified by the federal government as subject to sanctions, embargoes, and other restrictions.

Once a proposed relationship with a Sensitive Entity is identified, the faculty member who is responsible for the research activities with the Sensitive Entity, either as a host, principal investigator (PI), industrial affiliate, or in another assigned role on campus with the Sensitive Entity must take the following steps:

1. Meet with the Office of Research Integrity and Compliance and the Information Security Office to identify export control and information security risks involved in the project. UNT strongly recommends that projects with Sensitive Entities only generate public-domain research results. UNT does not recommend that projects with Sensitive Entities include research collaborations, visiting scholars affiliated with the Sensitive Entity, student internships, Sensitive Entity access to controlled or confidential data, Sensitive Entity involvement in federally sanctioned research centers, or projects that generate results intended to be kept confidential.

2. Notify in writing their Department Chair, the Division of International Affairs, as well as the Office of Research Integrity and Compliance and the Information Security Officer at least two weeks in advance of any proposed onsite activities involving visitors from the Sensitive Entity. If notice is received less than two weeks in advance of proposed activities, PI must obtain written approval from the Research Integrity and Compliance Office, the Information Security Officer, and either the Department Chair/Center Director or the Office of the Dean. In some cases, a plan may be required to supervise those visitors working with UNT research groups when the visitors are on campus. Onsite activities involving visitors from the Sensitive Entity are not permitted unless this notice is received.

3. Consult with UNT IT Security to determine if hardware or software provided or used by any representatives of the Sensitive Entity may enter the campus and be connected, locally or remotely, to the UNT network or any other UNT information resources, including university-owned laptops. Exceptions require written approval from the Information Security Office.

4. Complete the RIC/ISO Form and route for appropriate approvals to ensure that representatives of the Sensitive Entity are not issued a UNT EMPLID, provided any online account to any UNT information resource, provided remote access to any UNT information resources, or permitted access to use of UNT-owned laptops.

5. Complete COI and International Affiliations Disclosures to disclose support from and/or collaboration with the Sensitive Entity on proposals for federal research funding as required by the funding agency, particularly proposals that use the data generated during the project with the Sensitive Entity. UNT strongly recommends that the Sensitive Entity, and its employees and agents, are not involved as a consultant or subcontractor on federally funded projects.

6. Submit a Data Management Plan for the relationship with the Sensitive Entity for review and approval by the Office of Research Integrity and Compliance and the Information Security Office. The project will also be subject to review or audit to ensure that it is complying with the controls that are documented in the Data Management Plan.

7. Secure signatures from the Vice President for Research for all projects involving the Sensitive Entity approved by local boards or departments as a part of other research contracts or agreements.

8. Complete compliance training regarding international affiliations/export controls/COI and any other necessary trainings. All hosts, PIs, students, postdoctoral researchers, and staff who participate in the project must also complete such training.

Note: Outside the research domain, there may be instances when the Office of Research Integrity and Compliance and the Information Security Office identify a non-academic unit has proposed a business relationship with a Sensitive Entity. In those instances, the non-academic unit will be expected to work with the Research Integrity Office and to follow a modified versions of the steps listed above.

Definition of Sensitive Entity: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

GO TO PAGE 3 TO COMPLETE THE EXPORT AND SECURUTY RISK MANAGEMENT PLAN

Export and Information Security Risk Management Plan: Sensitive Entity

This form is used to document the actions required to mitigate the information security and export control risks created by a proposed relationship with a 'Sensitive Entity'. Please return this form, along with any supporting documents, to oric@unt.edu.

STEP 1: BASIC INFORMATION

UNT Responsible Individuals	

Sensitive Entity Information (To be completed by RIC)

Sanctioned Entity	
Sanctioning Authority	
Summary of Export Control Sanctions	
Sanctioned Individuals	
Agents of the Sanctioned Entity involved in the relationship	
Supporting Documents	

Description of Activity (To be completed by the host)

Nature of the Activity	
Dates of Activity	
Purpose of Activity	
Location of Activity	
UNT Resources	
Entity Resources	
Confidential Information	
Intellectual Property	
Research	
Export-Controlled Information or Research	
Supporting Documents	

STEP 2: Management Plan (To be completed by Host, RIC, RCA, ITSS)

The following actions are required to comply with the 'Memorandum on Relationships with Entities Identified as Presenting Elevated Export Control or Information Security Risks'.

Memo Requirement	Date of Completion	RIC/ECO Requirements
Discuss activity with the Research Integrity and Compliance Office (RIC) and Information Security Office (ECO) representative		
Notify the RIC and ECO at least two weeks in advance of any proposed onsite activities		
Write plan to supervise onsite visitors		
Prohibit use of the Entity's hardware or software on the UNT network		
Do not issue UNT EMPLIDs or provide access to UNT information resources (EMPLIDs)		
Disclose support and/or collaboration to federal funding agencies		
Submit Data Management Plan		
VPR approval for project agreements		
Export control and/or intellectual property protection training		
Post-monitoring Review		

STEP 3: Institutional Approvals

UNT Responsible Individuals

I have knowledge of the nature of the proposed activity, and the answers I have provided are true and correct to the best of my knowledge and belief. I understand that I must submit any changes in the nature or duration of the activity for prior approval to the Research Integrity and Compliance Office (RIC) and Information Security Office. I accept the responsibilities associated with conducting business with a Sensitive Entity and certify that I will make every reasonable effort to perform the actions required to mitigate the export control and information security risks created by the activity. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, export-controlled information, technology, software, or items to unauthorized persons.

Host:_____ Signature:_____ Date:_____

Department Chair:_____ Signature:_____ Date:_____

Information Security Office Representative

Recommend: Approval Disapproval

Name:_____ Signature:_____ Date:_____

Research Contracts and Agreements Office Representative

Recommend: Approval Disapproval

Name:_____ Signature:_____ Date:_____

Research Integrity and Compliance Office Representative

Export Licensing Determination:

Recommend: Approval Disapproval

Name:_____ Signature:_____ Date:_____