

Interim University Policy 4113: Research Security

Category: Academic Affairs

Subcategory: Research

Covered Individuals: Employees and Students

Responsible Executive: Vice President for Research

Policy Custodian: Office of Research; Chief Research Compliance Officer

Last Revised: 2026/10/27

Previous USU Policy Number: N/A

4113.1 PURPOSE AND SCOPE

This Policy addresses the efforts of foreign governments to use employees and students at U.S. universities to misappropriate, for economic and/or national security purposes, Research Data, as defined in [USU Policy 4107: Research Data](#), and intellectual property (IP). The concept of research security is designed to address such malign efforts.

This Policy integrates federal research security mandates, including but not limited to National Security Policy Memorandum 33 (2021), the CHIPS and Science Act (2022), and other federal agency-specific research security requirements for sponsored activities, into Utah State University (“USU” or “the University”) Policy.

This Policy establishes certain requirements and prohibitions for University employees and students in order to systematically and comprehensively mitigate foreign government-sponsored risks to University research efforts, which include, but are not limited to:

- An [International Activity and Collaboration](#) with a [High-Risk Entity](#) or one of its employees for research;
- An undisclosed International Activity and Collaboration in research with an entity based in or funded by a [Foreign Country of Concern](#) (FCOC);
- Participation in a [Malign Foreign Talent Recruitment Program](#) (MFTRP); and
- Transfer of University Research Data or IP to a High-Risk Entity or one of its employees.

Non-research activities involving High-Risk Entities, such as the contracts, agreements, or memoranda of understanding referenced in Section 2.3 of this Policy, have the potential to trigger adverse external action affecting University research, such as loss of federal funding and post-audit reporting requirements. Upon the future publication of additional University policy to address non-research activities involving High-Risk Entities, Section 2.3 of this Policy will be revised to apply exclusively to University Researchers and will no longer feature prohibited activity d, which addresses University contracts, agreements, or memoranda of understanding.

4113.2 POLICY

2.1 International Activities and Collaborations

Requirement to Disclose

All University employees and students who meet the definition of Researcher as defined in [USU Policy 4100: Research](#) ("University Researcher") and who are required to submit a conflict of interest disclosure under [USU Policy 2301: Individual Conflicts of Interest](#) must disclose to the University any International Activity and Collaboration as defined in Section 4113.6 of this Policy. University employees and students engaged in research must also disclose any International Activity and Collaboration on the appropriate disclosures to research sponsors.

Academic Affiliation

University Researchers who have a declared role, position, or appointment with a foreign entity may not exclusively affiliate themselves with that entity and must name Utah State University as an affiliation in their research activities, such as on publications or conference activities.

2.2 Malign Foreign Talent Recruitment Programs

University Researchers required to submit a conflict of interest disclosure as outlined in USU Policy 2301: Individual Conflicts of Interest must disclose participation in a foreign-sponsored transfer of knowledge or expertise to a foreign government, entity, or person—a [Foreign Talent Recruitment Program](#) as defined in Section 4113.6 of this Policy.

A Foreign Talent Recruitment Program becomes malign in nature—a Malign Foreign Talent Recruitment Program (MFTRP)—when it engages in problematic activity, such as the unauthorized transfer of intellectual property owned by the University or developed under a federal award. USU employees and students may not participate in any program that would meet the definition of a MFTRP under Section 4113.6 of this Policy during any period of their employment or student status with the University.

2.3 Prohibited Activities

University employees and students may not:

- a. Engage in any International Activity and Collaboration that involves a High-Risk Entity or employee of a High-Risk Entity, regardless of time and effort required for the activity and whether or not the University employee or student receives any form of compensation or benefit, financial or otherwise;
- b. Accept any form of compensation or benefit, financial or otherwise, from a High-Risk Entity or employee of a High-Risk Entity;
- c. Transfer University Research Data or intellectual property to a High-Risk Entity or employee of a High-Risk Entity; or
- d. Enter into any contract, agreement, or memorandum of understanding with a High-Risk Entity on behalf of the University.

Exception to Prohibited Activity A

Because the principal aim of research security is to prevent the misappropriation of USU Research Data and IP, especially when produced with federal funding, the Vice President for Research or one of their delegates may consider exceptions to prohibited activity a when:

- The proposed activity is limited to co-authorship and excludes all other activities defined under an International Activity and Collaboration; and
- The proposed activity (co-authorship) in no way involves research funded by a U.S. federal agency.

2.4 Activities Requiring Approval

University employees and students may not, without prior approval by the Vice President for Research or one of their delegates:

- a. Make University-Related Travel (URT), as defined under [USU Policy 5303: International Travel](#), to a FCOC; or

- b. Transfer University Research Data or intellectual property to an entity based in or funded by a FCOC.

2.5 International Travel

To allow the Office of Research to review international University-Related Travel for research security risk, University employees and students must adhere to [USU Policy 5303: International Travel](#), including by submitting a travel authorization and registering their travel for insurability.

As an approver in the travel authorization process, the Office of Research will not approve international URT involving any of the prohibited activities outlined in Section 4113.2.3 of this Policy.

For international URT presenting research security risk, the Office of Research will issue guidance to the traveling University employee or student.

University employees and students must follow any Office of Research-issued guidelines related to their international URT for research purposes.

2.6 Training and Certifications

When required by sponsors or the Office of Research, University employees and students will complete the University's designated version of Research Security Training, whether as a condition for submitting a proposal, for maintaining ongoing eligibility under an existing award, or both.

Learners will be automatically re-enrolled in Research Security Training on an annual basis until they indicate on a test-out question within the training that they are no longer on a federal award that requires the training and do not intend to seek additional federal funding in the foreseeable future.

When required by sponsors or the Office of Research, University Researchers will complete additional trainings and certifications, such as certification of non-participation in any Malign Foreign Talent Recruitment Program. When required by sponsors, the University will also complete institutional certifications and take the necessary steps, such as by initiating a Research Security Review, to confirm that its institutional certifications are accurate.

2.7 Research Security Reviews

To ensure compliance with this Policy, USU's Office of Research Integrity and Compliance (RIC), operating as a delegate of the Vice President for Research, will respond to any of the review triggers outlined in the Research Security Review Manual by initiating a Research Security Review of current and prospective USU employees, students, or external partners, collaborators, and visitors. The Office of Research may utilize both institutional data and third-party due diligence services to conduct its reviews.

Different risk factors identified in the Research Security Review will trigger different forms of mitigation. Each mitigation measure, as well as the general responsibilities of the relevant USU employees and students, is outlined in the Research Security Review Manual.

2.8 Non-Compliance

If the University finds non-compliance with any element of this Policy, USU employees and students may be subject to the ordinary disciplinary process of the University, such as the process outlined under the Faculty Code and the Student Code.

A University employee or student's failure to comply with any element of this Policy may also result in one or more actions consistent with applicable research agreements, sponsor requirements, and USU policies and procedures, including, but not limited to, modification, suspension, or termination of awards; required disclosures to awarding entities; exclusion from participation in specific research activities; imposition of additional oversight or management requirements; and/or other appropriate actions warranted under an associated research contract, law, regulation, or policy.

Federal Action

Federal entities, such as a research sponsor or law enforcement agency, may also penalize individuals and/or the University for non-compliance with this Policy through a number of means that include:

- Termination of federal awards and contracts;
- Suspension or debarment from eligibility for federal funding;
- Civil action, such as under the False Claims Act; and
- Arrest and/or criminal prosecution.

4113.3 RESPONSIBILITIES

3.1 University Employees and Students

Compliance with this Policy

To protect University Research Data and intellectual property, and to avoid outside scrutiny and legal consequences to themselves and the University, University employees and students must show a commitment to research security compliance by adhering to the aforementioned policies regarding training and certifications, disclosure of International Activities and Collaborations, non-participation in Malign Foreign Talent Recruitment Programs, non-participation in prohibited activities, travel to international destinations, and submitting certain research-related activities for approval.

Mitigation

University employees and students are responsible for complying with any sponsor- or University-issued mitigation measures for managing research security risk. The sponsor or the University may find a University employee or student ineligible for research activity, regardless of funding, for non-compliance with mitigation measures.

Duty to Report

University employees and students must report to the University (through the Office of Research) any suspected compromise of research security, such as, but not limited to, an undisclosed International Activity and Collaboration, participation in a Malign Foreign Talent Recruitment Program, and the unauthorized transfer of Research Data or IP to a foreign entity.

Duty to Cooperate

University employees and students must cooperate with the University's efforts to gather information, such as by conducting a Research Security Review, of a research security matter involving USU employees or students.

3.2 Principal Investigator

Principal Investigators, in addition to the responsibilities assigned to University employees and students under this Policy, face a heightened responsibility for research security compliance and must ensure that all people participating in any federal award are in compliance with the research security requirements of that award and/or governing agency, such as those relating to restricted entities, disclosure of research activities and sources of support, Research Security Training, and Malign Foreign Talent Recruitment Program certifications.

3.3 The University

To maintain the administrative functions necessary for University employees and students to follow every element of this Policy, the University will, where appropriate:

- Maintain this Policy in accordance with changes in research security best practices and federal requirements;
- Conduct fair and methodical risk reviews, such as through Research Security Reviews, of current and prospective USU employees, students, or external partners, visitors, or collaborators;
- Notify, when the University becomes aware and when appropriate, the University employees and students involved in activities involving research security risk and provide actionable guidance on mitigating such risk;
- Provision the appropriate University employees access to the internal and third-party tools necessary to conduct thorough, in-depth Research Security Reviews;
- Provision University employees and students with guidance and, when necessary, equipment to ensure that University Research Data and intellectual property are protected in the course of international travel;
- Make required trainings, such as Research Security Training, available to University employees and students;
- Notify employees and students of the research security requirements applicable to their research, such as those imposed by a specific funding agency;
- Notify external research partners of the research security requirements applicable to the research partnership in which the University is involved;
- Maintain a record of covered individuals' completion of required trainings, certifications, and disclosures that relate to research security;
- Certify to funding agencies institutional compliance with applicable research security requirements; and
- Work with funding agencies to implement project- or person-specific risk mitigation measures as required by those agencies.

Administrative Compliance

No University unit may administer or facilitate any activity that violates any element of this Policy. For example, the Sponsored Programs Office may not submit a proposal for funding on behalf of a University employee or student who has not taken a required Research Security Training, or the Controller's Office may not allocate funds to an activity that constitutes an activity requiring approval under Section 4113.2.4 of this Policy without prior approval by the Office of Research.

Duty to Report

The University will report, where deemed appropriate through coordination among the Office of Research, the Office of General Counsel, and any additional stakeholding University entities, research security violations or risk to the relevant research sponsors and law enforcement agencies.

4113.4 REFERENCES

- [National Security Policy Memorandum 33 \(NSPM-33\)](#), Presidential Memorandum on United States Government-Supported Research and Development National Security Policy, Presidential Memorandum, 14 January 2021.
- [Guidance for Implementing National Security Policy Memorandum 33 \(NSPM-33\) on National Security Strategy for United States Government-Supported Research and Development](#), National Science and Technology Council, January 2022.
- [Creating Helpful Incentives to Produce Semiconductors and Science \(CHIPS\) Act of 2022](#), Pub. L. No. 117-167, 136 Stat. 1366 (2022).

4113.5 RELATED USU POLICIES

- [Policy 2301: Individual Conflicts of Interest](#)
- [Policy 4100: Research](#)
- [Policy 4107: Research Data](#)
- [Policy 4109: Export Controls](#)
- [Policy 5303: International Travel](#)

Of the policies listed above, Policy 4109: Export Controls is the most closely intertwined with research security. Activities reviewed under this policy may also trigger U.S. export control requirements under Policy 4109, including a deemed export review, which apply in addition to, and independently of, the requirements of this policy.

4113.6 DEFINITIONS

Denied Person. A person who appears on the BIS Denied Persons List. For purposes of this policy, any person who appears on the BIS Denied Persons List is also considered a High-Risk Entity.

Foreign Country of Concern (FCOC). A country designated as a "foreign country of concern" under section 10638 of the CHIPS and Science Act of 2022, codified at 42 USC Sec. 19237(2), as amended. As of this Policy's last revision, the FCOCs so designated are the People's Republic of China (China), the Democratic People's Republic of Korea (North Korea), the Russian Federation (Russia), and the Islamic Republic of Iran (Iran).

Foreign Talent Recruitment Program. Any entity, program, or arrangement that facilitates compensation provided by a foreign state to a person in exchange for that person transferring knowledge and expertise to a foreign country, an institution based in that foreign country, or citizens of that foreign country.

High-Risk Entity. Any entity appearing on a U.S. government restricted or prohibited party or entity list used for national security, export controls, or sanctions compliance, or a list published for the same purpose by a non-governmental entity generally credible on academic and/or national security matters, such as the National Academies of Sciences, namely:

- Sec. 1260H of the *National Defense Authorization Act* (NDAA) for FY2021 (U.S. Department of Defense);
- Sec. 1286 of the NDAA for FY2019 (U.S. Department of Defense);
- Sec. 889 of the NDAA for FY2019 (U.S. Department of Defense, U.S. General Services Administration, National Aeronautics and Space Administration);
- Sec. 5949 of the NDAA for FY2023 (U.S. Department of Defense, U.S. General Services Administration, National Aeronautics and Space Administration);
- Entity List (U.S. Department of Commerce, Bureau of Industry and Security);
- Military End-User Entities (U.S. Department of Commerce, Bureau of Industry and Security);
- Denied Persons (U.S. Department of Commerce, Bureau of Industry and Security);
- Specially Designated Nationals List (U.S. Department of Treasury, Office of Foreign Assets Control);
- Annex of Executive Order 14032 (U.S. Department of Treasury, Office of Foreign Assets Control);
- Non-SDN Chinese Military-Industrial Complex Companies (U.S. Department of Treasury, Office of Foreign Assets Control);
- Debarred Parties (U.S. Department of State);
- Nonproliferation Sanctions (U.S. Department of State);
- Equipment and Services Covered by Section 2 of The Secure Networks Act (U.S. Federal Communications Commission);
- UFLPA Entity List (U.S. Department of Homeland Security);
- Withhold Release Orders & Findings (U.S. Department of Homeland Security, Customs and Border Protection);
- Foreign Talent Programs That May Pose a Threat to the National Security Interests of the United States (National Academies of Sciences); and
- China's Defense S&T Key Lab System (U.S. Department of Defense, U.S. Air Force, China Aerospace Studies Institute).

International Activity and Collaboration. Any:

- role, position, or appointment with a foreign entity, whether full-time, part-time, or voluntary and whether or not the activity results in a form of compensation or benefit, financial or otherwise;
- collaboration in the form of co-investigator status on a project, an advisor/advisee role, co-authorship,

or any other direct relationship within a professional scholarly setting designed to produce a research outcome; or

- use of facilities, instrumentation, laboratories, field sites, or other research infrastructure located at a foreign site.

Malign Foreign Talent Recruitment Program (MFTRP). A program labeled a malign foreign talent recruitment program or a foreign talent recruitment program that may pose a risk to the national security interests of the United States by a third-party, non-governmental entity generally credible on academic and/or national security matters, such as, but not limited to, the National Academies of Sciences; or, as defined in 42 USC Sec 19237(4):

(A) any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to the targeted individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue, in exchange for the individual—

- (i) engaging in the unauthorized transfer of intellectual property, materials, data products, or other nonpublic information owned by a United States entity or developed with a Federal research and development award to the government of a foreign country or an entity based in, funded by, or affiliated with a foreign country regardless of whether that government or entity provided support for the development of the intellectual property, materials, or data products;
- (ii) being required to recruit trainees or researchers to enroll in such program, position, or activity;
- (iii) establishing a laboratory or company, accepting a faculty position, or undertaking any other employment or appointment in a foreign country or with an entity based in, funded by, or affiliated with a foreign country if such activities are in violation of the standard terms and conditions of a Federal research and development award;
- (iv) being unable to terminate the foreign talent recruitment program contract or agreement except in extraordinary circumstances;
- (v) through funding or effort related to the foreign talent recruitment program, being limited in the capacity to carry out a research and development award or required to engage in work that would result in substantial overlap or duplication with a Federal research and development award;
- (vi) being required to apply for and successfully receive funding from the sponsoring foreign government's funding agencies with the sponsoring foreign organization as the recipient;
- (vii) being required to omit acknowledgment of the recipient institution with which the individual is affiliated, or the Federal research agency sponsoring the research and development award, contrary to the institutional policies or standard terms and conditions of the Federal research and development award;
- (viii) being required to not disclose to the Federal research agency or employing institution the participation of such individual in such program, position, or activity; or
- (ix) having a conflict of interest or conflict of commitment contrary to the standard terms and conditions of the Federal research and development award; and

(B) a program that is sponsored by—

- (i) a foreign country of concern or an entity based in a foreign country of concern, whether or not directly sponsored by the foreign country of concern;
- (ii) an academic institution on the most recent list developed under section 1286(c)(8) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note; Public Law 115–232) or such other list developed by the Federal Government to replace this list; or a foreign talent recruitment program on the most recent list developed under section 1286(c)(9) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note; Public Law 115–232) or such other list as may be developed by the Federal Government to replace this list.

Information below is not included as part of the contents of the official policy. It is provided only as a convenience for readers/users and may be changed at any time by persons authorized by the President.

RESOURCES

Guidance

- [Research Security Review Manual](#)
- [Research Security Training, USU Office of Research](#)
- [Foreign Talent Recruitment Programs, USU Office of Research](#)
- [Federal Research Security Reporting and Certification Requirements, USU Office of Research](#)

Related Forms and Tools

- [Research Security Self-Check Tool](#)

Contacts

- Compliance Officer
Research Integrity & Compliance
research.usu.edu/compliance
compliance@usu.edu

POLICY HISTORY

Original issue date: 2026/10/27

Last revision date: 2026/10/27

Next scheduled review date: 2027/10/01

Previous revision dates: N/A