ADMINISTRATIVE DIVISION	RSCH Office of Research
POLICY NUMBER	RSCH 1.12
POLICY TITLE	Research Security
SCOPE OF POLICY	USC System
DATE OF REVISION	April 14, 2026
RESPONSIBLE OFFICER	Vice President for Research
ADMINISTRATIVE OFFICE	Office of Research

PURPOSE

This policy establishes the University's Research Security Program (RSP) in alignment with federal mandates, including National Security Presidential Memorandum 33 (NSPM-33), the CHIPS and Science Act of 2022, and related agency guidance. The RSP is designed to safeguard the integrity, confidentiality, and security of the University's research enterprise while fostering an open and collaborative academic environment.

DEFINITIONS

Covered Individuals: An individual who contributes in a substantive, meaningful way to the scientific development or execution of a research and development project proposed to be carried out with a research and development award from a federal research agency or designated as Key Personnel or Covered Individual by the federal research agency concerned.

Foreign Countries of Concern
A Foreign Country of Concern (FCOC) is a country that is a covered nation (as defined in section 4872(d) of title 10 United States Code); and (B) any country that the Secretary, in consultation with the Secretary of Defense, the Secretary of State, and the Director of National Intelligence, determines to be engaged in conduct that is detrimental to the national security or foreign policy of the United States.

Research Security: Safeguarding the research enterprise against the misappropriation of research results and resources to the detriment of national or economic security.

Research Collaboration: Multiple parties working together on a defined project and sharing resources, materials, data, information, intellectual property, and/or expertise to achieve shared research goal(s).

POLICY STATEMENT

I. University Responsibilities

The University is committed to promoting a secure research environment that protects against undue foreign influence, intellectual property theft, and unauthorized disclosure of sensitive,

restricted, or controlled research data. In accordance with NSPM-33 and subsequent federal guidance, the University shall implement and maintain a comprehensive Research Security Program that addresses the following institutional responsibilities:

1. **Cybersecurity**
   Information Technology (IT) teams with primary responsibility for networks or systems within their respective organizational units (OUs) are responsible for implementing and maintaining controls (including safeguards and protections) required by the United States Government (USG) and their sponsor agencies. Such controls must be appropriate for the classification level of the research information being processed, stored, or distributed in a particular network or system. Additionally, supplemental university policies including IT 1.00 – Information Technology Procurement and IT 3.00 – Information Security provide additional information.

2. **Foreign Travel Security**
   The University shall provide pre-travel briefings, risk guidance, and resources to Covered Individuals engaged in research-related international travel to mitigate risks associated with foreign interference, exploitation, and data loss.

3. **Training**
   The University shall develop, implement, track, and document required research security and export control training consistent with USG and sponsor agency requirements.

4. **Export Control Compliance**
   The University will ensure compliance with U.S. export control laws and regulations.

5. **Disclosure and Transparency**
   The University shall establish mechanisms for the collection, review, management, and certification of required disclosures related to foreign affiliations, support, outside activities, and financial interests in accordance with sponsor requirements and institutional policies, including: RSCH 1.06 - Disclosure of Financial Interests and Management of Conflicts of Interest Related to Sponsored Projects, ACAF 1.50 - Outside Professional Activities for Faculty, and BTRU 1.18 - Conflicts of Interest and Commitment.

6. **Governance and Oversight**
   The Office of Research will designate a Chief Research Security Officer responsible for program implementation, monitoring, and institutional certification.

II. Covered Individual Responsibilities

Covered Individuals are responsible for complying with all applicable research security requirements and institutional policies. Specifically, Covered Individuals shall:

1. **Cybersecurity**

Comply with institutional cybersecurity controls and safeguard research data in accordance with applicable classification and sponsor requirements.

2. **Foreign Travel Security**
   Participate in required pre-travel briefings and adhere to institutional guidance regarding secure international travel and protection of research data and devices.

3. **Required Training**
   Complete all required research security, export control, and related compliance training within designated timeframes and maintain current certification status.

4. **Export Control Adherence**
   Consult with appropriate university offices prior to engaging in activities involving controlled technologies, international shipments, restricted parties, or sanctioned countries to ensure compliance with U.S. export control laws and regulations.

5. **Disclosure and Transparency**
   All researchers must disclose foreign affiliations, support, and activities as required by federal sponsors and institutional policy including RSCH 1.06 - Disclosure of Financial Interests and Management of Conflicts of Interest Related to Sponsored Projects, ACAF 1.50 - Outside Professional Activities for Faculty, and BTRU 1.18 - Conflicts of Interest and Commitment.

PROCEDURES

The Office of Research Security (ORS), under the oversight of the Vice President for Research (VPR) and led by the Chief Research Security Officer (CRSO), is responsible for administering the Research Security Program (RSP). For more information on the office and the Research Security Program, visit the research security website at: Office of Research Security - Office of the Vice President for Research | University of South Carolina

The related policies and regulations listed below provide a comprehensive framework that reinforces the research security policy. They address key areas such as intellectual property, information security, conflicts of interest, foreign travel authorization, compliance with foreign affiliations and export controls. These policies ensure that all research activities are conducted with integrity, transparency, and adherence to regulatory requirements, thereby safeguarding the university's interests and supporting responsible research practices.

RELATED UNIVERSITY, STATE AND FEDERAL POLICIES

- ACAF 1.33 – Intellectual Property
- ACAF 1.50 - Outside Professional Activities for Faculty
- BTRU 1.18 - Conflicts of Interest and Commitment
- FINA 1.50 – Foreign Gift and Contract Reporting

- IT 1.00 – Information Technology Procurement
- IT 3.00 – Information Security
- RSCH 1.00 – Misconduct in Research and Scholarship
- RSCH 1.05 – Data Access, Retention and Ownership
- RSCH 1.06 - Disclosure of Financial Interests and Management of Conflicts of Interest Related to Sponsored Projects
- RSCH 1.10 - Prohibition of Participation in Malign Foreign Talent Recruitment
- UNIV 1.51 – Data and Information Governance
- UNIV 1.52 – Responsible Use of Data, Technology and User Credentials
- National Security Presidential Memorandum 33 (NSPM-33)
- FINA 2.50 - Travel
- NSPM-33 Implementation Guidelines
- The Chips and Sciences Act

HISTORY OF REVISIONS

DATE OF REVISION	**REASON FOR REVISION**
April 14, 2026	New policy approval