RESEARCH SECURITY AND COMPLIANCE

AT A GLANCE

Research Security and Compliance (RSC) is about protecting the integrity, confidentiality, and value of research. RSC ensures the people, ideas, data, and technologies involved in research are safe from theft, misuse, or interference - whether that's from cyber threats, insider risks, or even foreign influence.

RSC's purpose is to create a secure environment where researchers can collaborate, innovate, and share knowledge responsibly. That includes things like:

- Protecting sensitive data *(like proprietary findings, export controlled information, Controlled Unclassified Information)*
- Ensuring compliance with laws and funding agency requirements
- Safeguarding intellectual property
- Preventing malign foreign influence or espionage

TWO TYPES OF RESEARCH:

FUNDAMENTAL RESEARCH

NOTE: *The legal definition of Fundamental Research differs from the more widely accepted and known definition used within the scientific community.*

Fundamental Research: Research in basic or applied science and engineering where the resulting information is intended to be published.

University research will not be considered fundamental if:

- The University, or its researchers, accept restrictions on publication of scientific and technical information resulting from the project or activity; or
- The research has specific access and dissemination controls preventing access based on citizenship or nationality.

Fundamental Research does not apply to

- Equipment, software or technology used to conduct research; or
- Tangible items that result from research.

CONTROLLED RESEARCH

Controlled Research

If research is not Fundamental Research, it will be considered Controlled Research and will be subject to U.S. export control regulations. Reach out to our office for guidance on including a Fundamental Research statement in your proposal and addressing restrictive clauses.

Indicators of Controlled Research will very likely include mentions of the following: Export Controlled, International Traffic in Arms Regulation (**ITAR**), Export Administration Regulations (**EAR**), Controlled Unclassified Information (**CUI**), Covered Defense Information (**CDI**), Controlled Technical Information (**CTI**), Cybersecurity Maturity Model Certification (**CMMC**), **NIST 800-171**, **DFARS,** or Distribution Statement.

POINTS FOR CONSIDERATION:

- Security protocols in your grant proposals (*including budgeting*).
- Training may be required prior to the submission of research proposals.
- Laboratory space may need additional security when conducting controlled research.
- Research funding may be delayed if required controls aren’t put in place prior to executing research contracts.
- International travel and shipping may require an export authorization.
- Foreign persons may require an export authorization for information shared with them even when in the U.S., if controlled.

SANCTIONED AND FOREIGN COUNTRIES OF CONCERN

Collaborating or researching with sponsors, institutions or researchers located in the following countries require additional due diligence from Research Security and Compliance.

Foreign Countries of Concern:

China - including Hong Kong & Macau

North Korea

Iran

Russia

Comprehensively Sanctioned Countries:

Cuba

North Korea

Iran

Russian-occupied regions of Ukraine

Syria

CONTACT RESEARCH SECURITY OFFICE

Proactively reaching out to the RSC team early in the solicitation/proposal process can save you time and money. Controlled Research has unique funding requirements and RSC is here to help!

✉ JOE FLERI, DIRECTOR FOR RESEARCH SECURITY AND COMPLIANCE
JFLERI@UMSYSTEM.EDU

WWW.UMSYSTEM.EDU/UMS/ECAS/RESEARCH

University of Missouri System