Research Security and Compliance

University of Missouri-Columbia

Standard Operating Procedure
Training and Awareness

Training and Awareness

Effective Date: February 1, 2025
Original Approval Date: January 23, 2025
Revised Date: N/A

Approved By: Michele Kennett
Associate Vice Chancellor for Research

Table of Contents

1.0   Purpose

The University of Missouri-Columbia (MU) must comply with U.S. export control and sanctions regulations, safeguarding requirements for Controlled Unclassified Information (CUI), and general research security training requirements. Outreach and education through targeted and risk-based trainings will be facilitated by a member of the Research Security and Compliance (RSC) staff. The objective is to ensure that appropriate personnel at MU understand the institution's regulatory compliance requirements and the relevant administrative review and safeguarding processes that are associated with meeting export controls and sanctions regulations, CUI safeguarding obligations, and general research security training requirements.

2.0   Scope

This SOP formalizes training responsibilities for RSC staff and other appropriate personnel at MU.

3.0   Responsibilities

RSC will provide training, outreach, and education on export control and sanctions regulations to MU personnel in risk sensitive areas identified by RSC. Training is to help MU personnel understand their obligations under the export controls and sanctions and research security program at MU. RSC will ensure CUI trainings are completed by those with access to CUI. RSC will work with Sponsored Programs Administration (SPA) on the implementation of research security training requirements pursuant to National Security Presidential Memorandum-33, the CHIPS and Science Act of 2022, and related implementation required by federal funding agencies.

Responsibilities of RSC

a. Ensure that personnel within administrative areas at MU, that have responsibilities for flagging items to RSC for review, receive annual training on export controls and sanctions risks and on the specific operational requirements related to the reviews undertaken by their administrative area.

b. Ensure that all MU personnel who are granted access to export controlled information receive briefings at least once every 3 years that are specific to their responsibilities when handling export controlled information. If there are significant changes to a Technology Control Plan (TCP) or significant changes to the regulations, RSC may need to provide training more frequently.

c. Ensure that MU personnel who will access CUI complete annual CUI training.
d. Support ad hoc requests for additional trainings or briefings when requested by MU leadership, faculty, staff, and students.
e. When identified by RSC, provide additional training(s) that may be required for MU personnel accessing export controlled information, CUI, or other related sensitive or critical information, such as Operations Security training, required at an appropriate frequency as determined by RSC.
f. Work with SPA to ensure that general research security training requirements are implemented pursuant to National Security Presidential Memorandum-33, the CHIPS and Science Act of 2022, and related implementation requirements of federal funding agencies.

Responsibilities of MU personnel within risk sensitive administrative areas
a. Complete briefings and trainings as required by RSC.
b. Ask questions and seek clarification for any portions of the training.
c. Notify RSC if there are any new people in the unit requiring training, between annual trainings, so that RSC can facilitate training as part of onboarding.

Responsibilities of MU personnel with access to export controlled information and/or CUI
a. Complete briefings and trainings as required by RSC.
b. Ask questions and seek clarification for any portions of the training.
c. Take individual responsibility to understand the frequency of training requirements and take initiative to proactively complete training on their own or when reminded to complete annual refresher training by RSC.

Responsibilities of MU personnel that require additional relevant training
a. Complete briefings and trainings as required by RSC.
b. Ask questions and seek clarification for any portions of the training.
c. Take individual responsibility to understand the frequency of required training and take initiative to proactively complete training on their own or when reminded to complete annual refresher training by RSC.

Responsibilities of MU personnel required to complete general research security training
a. Complete trainings as required by RSC and/or SPA
b. Ask questions and seek clarification for any portions of the training.
c. Take individual responsibility to understand the frequency of training requirements and take initiative to proactively complete training on their own or when reminded to complete annual refresher training by RSC or SPA.

4.0   Procedure
Training for personnel within risk sensitive administrative areas
S1. Prior to annual training, RSC will partner with the leader of relevant administrative unit(s) to review existing procedures and assess if there are there any necessary changes to procedures.
a. If yes, RSC and the leader of the relevant administrative unit(s) will review and edit the SOP together and obtain any required institutional signatures. Move to S2 once any SOP updates are complete.
b. If no changes, move to S2.

S2. RSC partners with the leader of each administrative unit to schedule a time for the training and prepares a training presentation specific to the SOP in place for that unit.

S3. RSC meets with the unit to facilitate the training and maintains records of the training in accordance with RSC recordkeeping procedures.

S4. RSC creates a reminder for the following year to review the SOP again and repeat this process.

Training for personnel with access to export controlled information
S1. RSC will ensure that a TCP briefing is provided as part of the TCP onboarding process prior to receiving access to export controlled information.

S2. RSC maintains records of the briefing in accordance with RSC recordkeeping procedures.

S3. RSC reviews training records when completing TCP audits to identify if anyone's briefing is past-due or will be past-due at some point in the calendar year of the audit, and provides a refresher briefing, as needed.

S4. If a refresher TCP briefing is not completed within 30-days of the initial request, access to export controlled information will be removed until completion of the training requirement.

Training for personnel with access to CUI
S1. RSC will ensure that CUI training is completed by all personnel as part of the TCP onboarding process and prior to receiving access to CUI.

S2. RSC will maintain records of the training in accordance with RSC recordkeeping procedures.

S3. RSC will review training records when completing TCP audits to identify if anyone's briefing is past-due or will be past-due at some point in the calendar year of the audit, and requires a refresher training, as needed.

S3. If refresher CUI training is not completed by personnel within 30-days of the initial request, access to CUI will be removed until completion of the training requirement.

Additional training for relevant personnel as determined by RSC
S1. RSC will identify the need for any additional training needs, such as Operations Security training, based on sponsor requirements or other risks as identified by RSC.

S2. RSC will ensure that all personnel with a need to complete additional training will complete said training and record that training in accordance with the RSC recordkeeping procedures.

S3. RSC will review training records when completing TCP audits to identify if anyone's additional required training is past-due or will be past-due at some point in the calendar year of the audit, and requires a refresher training, as needed.

S4. If training is not completed within 30-days of the initial request, access to export controlled information, CUI, or other related sensitive or critical information will be removed until the completion of the training requirement.

Research security training as required by federal funding agencies as a condition of federally funded sponsored research proposals and/or awards
S1. RSC and SPA personnel will identify the need for research security training, as required by National Security Presidential Memorandum-33, the CHIPS and Science Act of 2022, and related implementation by federal funding agencies.

S2. SPA and/or Department personnel will ensure that all MU personnel that need to complete research security training will complete said training at proposal or award, depending on specific federal funding agency requirements.

S2. If training is not completed in a timely manner in accordance with specific federal funding agency deadlines, SPA may be unable to submit proposals or execute awards until training is up to date.