Training Requirements for Participation in Federally Sponsored Research

Office of Research
Policy Number: 1.7

Effective Date: Fall 2025
Last Update: Fall 2025

I. Policy Summary

This policy provides guidelines for the training requirements for sponsored projects for all senior and key personnel at the New Jersey Institute of Technology ("NJIT") that extend beyond the general responsible conduct of research (RCR) training detailed in Research Policy 1.2.

II. Policy Purpose

The purpose of this policy is to outline the training requirements and internal process for NJIT personnel involved in proposals or awards that are subject to federal regulations.

III. Policy Scope and Applicability

This policy is in effect for all units of NJIT and applies to all sponsored programs.

IV. Definitions

The following definitions shape the guidance regarding required training:

The CITI Research Security Advanced course contains eight modules:

- Introduction to Research Security – This first module introduces research security with a historical context of research security initiatives, including NSPM-33 and the CHIPS and Science Act. The module provides an overview of the new requirements that researchers and compliance officers will be expected to meet. The module concludes with best practices that researchers can follow to protect themselves.
- Risk Mitigation and Research Security – This module begins with a review of the U.S. government's research security concerns as they relate to research and development. Learners will explore researchers' responsibilities for risk mitigation, including practical approaches for international collaborations, insider threats, and engaging institutional resources. The module concludes with a discussion of additional resources to help individuals navigate the challenges that research security threats present.
- Cybersecurity and Research Security – Cybersecurity is a critical issue across organizations. This module provides a summary of fundamental cybersecurity elements, recognizing that individuals are often required to complete cybersecurity training content throughout the year as part of a larger enterprise security program. The module provides learners with a discussion of cybersecurity as it applies to research, including examples of research security controls. It concludes by touching on the intermediate-level topics of controlled unclassified information and the Cybersecurity Maturity Model Certification (CMMC).
- International Collaborations – International collaborations play an essential role in the advancement of research. This module examines the various ways researchers collaborate and outlines key elements to consider when engaging in collaborative relationships. Learners will explore the unique risks associated with international collaborations and understand the intersection of laws, policies, and stakeholders that guide such collaborations. The module concludes with a review of internal and external resources to

help minimize risk.

- International Travel – This module provides an overview of security risks associated with international travel. The module enables learners to consider situations that require additional approvals from their organizations, U.S. government agencies, or other relevant governments/authorities related to international travel. Traveling with electronic devices or data is often a necessary aspect of research-related travel. This module explores standard methods for securing electronic devices and data. The module concludes with a review of internal and external resources to help minimize security risks.
- Foreign Interference – Foreign interference in research remains a concern for the U.S. government as well as research organizations. This module begins with a review of the importance of knowing collaborators and parties with whom researchers may work. It explores the characteristics of "entities" and "countries of concern," as well as indicators of "malign" foreign talent recruitment programs. The module concludes with a review of the consequences of working with such entities, as well as strategies for minimizing risks and available resources.
- Federal Funding & Foreign Gifts and Contracts – This module reviews the requirements and impacts of NSPM-33 and the CHIPS and Science Act for researchers and recipient institutions, including the reporting of foreign gifts and contracts. The module also describes how the appropriate use of federal funds aligns with research security and the requirements of key federal research funding agencies regarding non-U.S. activities.
- Disclosures and Transparency -- This module provides learners with a review of the rationale for disclosure and transparency in relation to scientific integrity and in the research proposal and award process. Learners will review who is required to disclose, what information must be disclosed to the institution and to federal sponsors, and the various mechanisms and methods used to complete disclosure. Note: This module was updated in September 2025 to comply with the NIH requirements for disclosure of other support.

V. Policy Statement

To be in compliance with federal regulations for all agencies (e.g., NSF, NIH, etc.) all senior and key personnel included in sponsored funding must complete the required training annually. This annual training must be completed within 12 months of a proposal submission date and any personnel joining a project will be required to take the training before they can be added to the project. The training requirements will be updated regularly in response to need and changes in regulations. Currently, federal agencies set expectations about training and policies separately, and this policy aims to be broad and apply to all agencies.

VI. Procedures

All senior and key personnel take the CITI course titled "Research Security Advanced" on time.

VII. Roles & Responsibilities

- Senior and key personnel
  - Take the CITI course "Research Security Advanced" promptly.
- Pre-award services
  - Confirm senior and key personnel have taken the required training before submission.
  - Proposals will not be submitted if the training is not taken within 12 months of submission for all known senior and key personnel.
- Research Compliance
  - Send reminders about post submission training for senior and key personnel added after submission, and for all to have the training at least once in the 12 months after submission.

VIII. Authority and Responsibility

The Office of Research has institutional authority for the matters addressed in this policy. Questions related to this policy are to be directed to the Office of Research.