Category: Administrative **Program applicable** Faculty/Staff/Students	*Policy Title:* **Insider Threat Program – Classified Research** **Effective Date:** 07/01/2025 **Prior Effective Dates:** **Enabling Acts:** 32 CFR Part 117 Board Rule 10-30-04	*Policy Number:* 1.9.13 **Policy Owner:** VP for Research **Responsible Office(s):** Research Security and Ethics Office of Research

1. Purpose.

This plan establishes policy and assigns responsibilities for the University of Cincinnati (UC) Classified Insider Threat Program (CITP). The CITP will establish a program to gather, evaluate and report relevant and credible information that may be indicative of a potential or actual Insider Threat. An Insider Threat is defined by The National Industrial Security Program Operating Manual (NISPOM), codified in 32 CFR Part 117, as, "the likelihood, risk or potential that an insider will use his or her authorized access, wittingly or unwittingly to do harm to the national security of the United States." Insider Threats may result in harm to UC or U.S. program information, to the extent that the information impacts UC's obligations to protect classified national security information.

2. Scope and applicability.

The CITP applies to all UC entities and personnel with authorized access to any classified U.S. government or UC resources, including personnel, facilities, information, equipment, networks, or systems.

3. Policy.

The purpose of the CITP is to protect personnel, facilities, and automated systems from insider threats in compliance with the NISPOM. The CITP will meet or exceed the minimum standards for such programs consistent with guidance provided in Industrial Security Letter (ISL) 2016-02 and the Defense Counterintelligence and Security Agency (DCSA) Assessment and Authorization Process Manual for Certification and Accreditation of Classified Systems under the NISPOM.

This program will seek to

- Prevent espionage or the unauthorized disclosure of classified information;

- Deter cleared employees granted personnel clearances (PCLs) and employees being processed for PCLs from becoming insider threats;
- Detect any cleared person with authorized access to any government or UC resources to include personnel, facilities, information, equipment, networks, or systems, who pose a risk to classified systems and classified information; and
- Mitigate the risks to the security of classified information through administrative, investigative, or other responses or any combination of these processes.

The responsibilities outlined below are designed to enable the Insider Threat Program Senior Official (ITPSO) to collaborate with the Insider Threat Working Group (ITWG) to gather, evaluate, centrally analyze, and respond appropriately to key threat-related information. The ITWG will consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, and civil liberties issues including, but not limited to, the use of personally identifiable information, are appropriately addressed.

4. Definitions

Assets: Assets include human capital, collateral materials, intellectual property, U.S. National Security information, information technology systems and equipment, the secret compartment space, and U.S. government sensitive information.

Classified Information: As defined in the Classified Information Procedures Act 1980, any information or material that has been determined by the U.S. government, pursuant to an executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).

Cleared Personnel: Employees whose clearance is held by UC with authorized access to any U.S. Government (USG) or university resource, including personnel, facilities, information, equipment, networks, and systems.[1]

Insider Threat: An insider threat is the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to UC or U.S. program information, to the extent that the information impacts UC or the U.S. government's obligations to protect classified national security information. Insider threats may be posed by a current or former employee, or consultant, who has or has had authorized access to sensitive information and assets protected by UC, who intentionally or unintentionally misuses that access in a manner which negatively affects the confidentiality, integrity or availability of classified information or related UC operations, resources, or other assets.

[1] University personnel whose clearances are managed by an outside organization, but not by UC, are not considered Cleared Personnel for the purposes of this program. **[This is fine if such personnel will not have access to classified information at UC.]**

5. Responsibilities

a. Senior Management Official (SMO)[2]

In accordance with § 117.7 (b)(2) of the NISPOM Rule, the SMO:

(1) Shall formally (in writing) appoint an Insider Threat Program Senior Official (ITPSO) for UC. The ITPSO must be a U.S. Citizen and have eligibility to maintain a personnel security clearance (PCL) at the same level as the UC facility security clearance (FCL). The ITPSO can be the Facility Security Officer (FSO).

(2) Ensure the FSO maintains a system of security controls in accordance with the requirements of the NISPOM rule.

(3) Remain fully informed of the facility's classified operations.

(4) Make decisions based on classified threat reporting and their thorough knowledge, understanding and appreciation of the threat information and the potential impacts caused by a loss of classified information.

b. Insider Threat Program Senior Official (ITPSO)

The ITPSO shall:

(1) Complete the training required by 32 CFR § 117.7(b)(4)(ii).

(2) Establish, execute and provide management, accountability, and oversight of the ITP.

(3) Chair and convene the UC ITP Working Group (ITWG).

(4) Oversee the collection, analysis, and reporting of information across the university to support the identification and assessment of Insider Threats.

(5) Develop annual ITP training requirements for the ITWG members and Cleared Personnel that will meet or exceed the requirements outlined in paragraph § 117.12(g) of the NISPOM Rule.

(6) Shall establish and manage the program via an encrypted enclave for the ITP that limits access to only ITWG members and Cleared Personnel.

(7) The ITPSO will ensure that the FSO is an integral member of UC's implementation of the ITP (32 CFR § 117.7(b)(4)(i)).

(8) Establish and manage all implementation and reporting requirements related to the ITP, including self-assessments and independent assessments, the results of which shall be reported to the SMO in a timely manner.

c. Insider Threat Working Group (ITWG)

(1) The ITWG will be chaired by the ITPSO, and shall consist of the following individuals or individuals representing the following offices, as applicable:

a. FSO

[2] The SMO for UC is the University President.

b. Central Human Resources
c. Office of Information Security
d. Office of General Counsel
e. Research Security and Ethics
f. Privacy Officer
g. Law Enforcement Office

(2) The ITPSO may add additional members to the ITWG as needed to ensure the ITWG can fulfill the purpose of the CITP as described in Paragraph 1, above.

(3) The ITWG will meet no less than annually and as needed to discuss any issues or incidents involving Cleared Personnel that may pose an Insider Threat. The ITWG will develop recommendations to prevent and mitigate Insider Threats.

The ITWG will assist the ITPSO with security inquiries concerning potential Insider Threats reported by Information Security personnel by obtaining and providing necessary information to determine if the information or allegations are credible and should be referred to the U.S. government for further investigation in consultation with Office of General Counsel.

d. ITWG Members' Responsibilities

Each ITWG member shall:

(1) Provide expertise relevant to the CITP to the ITWG concerning their area of responsibility.

(2) Report violations, compliance issues or incidents that include relevant and credible Insider Threat information related to the Adjudicative Guidelines involving Cleared Personnel to the ITPSO.

(3) Provide information related to observed trends relevant to Insider Threats in their respective area of responsibility.

(4) Participate in and complete CITP training as determined by the ITPSO.

e. UC Cleared Personnel Responsibilities

(1) Report suspected or actual Insider Threat related issues related to the Adjudicative Guidelines involving other Cleared Personnel to the ITPSO and/or FSO. If such issues are reported to the FSO, then the FSO shall promptly notify the ITPSO.

(2) Self-report any adverse information or issues that may relate to the Adjudicative Guidelines.

(3) Participate in annual CITP training as determined by the ITPSO.

6. Procedures

a. Indoctrination Cleared Personnel into UC's security program

(1) FSO will evaluate, in accordance with Board Rule 10-30-04, new requests for UC participation in classified research programs to confirm. that the granting of such request would not pose an Insider Threat. Any such Insider Threat shall be reported to the ITWG.

(2) The FSO shall ensure that the ITWG is kept up-to-date on the list of classified research programs being conducted at UC, as well as a list of Cleared Personnel associated with each program. Updates to the ITWG shall be provided via the encrypted enclave.

b. Monitoring and reporting of ITP incidents

(1) ITWG members will periodically review the records in their areas of responsibility for any Insider Threat issues related to Cleared Personnel in the context of the Adjudicative Guidelines and will provide a report back to the FSO and ITPSO when credible derogatory information is discovered, no less than annually.

(2) If an incident is reported, the appropriate ITWG member shall compile an initial summary of the incident and report to the ITPSO via the encrypted enclave.

(3) ITWG members will review quarterly reports developed from the University's Electronic Communications Monitoring Program as well as incident reports submitted pursuant to (c) below.

c. Processing an ITP incident report

(1) ITPSO shall prepare an CITP incident report for each incident reported to the ITPSO, whether by a member of the ITWG or otherwise, to include the following information:

a) A unique, but deidentified header, preserving the anonymity of the subject;

b) Summary of any past incidents involving the subject;

c) Description of incident and relevant Adjudicative Guideline(s) and any steps already taken; and

d) A recommended course of action, which could be any of the following:

1. File within the subject's personal security record maintained by the FSO and Report to the Defense Counterintelligence and Security Agency (DCSA), UC's Cognizant Security Office (CSO). If subject is cleared through another agency, report the issue to their relevant office as well.
2. File within subject's personal security record, but do not report to CSO.
3. Do not file within the subject's personal security record.
4. Any additional action up to and including revocation of subject's access to UC's classified information and removal from the UC's security program.

(2) The ITPSO will share CITP incident reports with the ITWG.

(3) All ITWG members shall indicate their agreement or disagreement with the ITPSO's recommendation.

a) If all ITWG members agree, the recommendation shall be implemented.

b) If there are any dissenting opinions, the ITPSO shall schedule an ITWG meeting to discuss the incident and determine the course of action.

c) The final decision shall be reported to the SMO, and DCSA as required.

d. Meetings - The ITWG will meet no less than annually and as needed to discuss the following:

(1) A summary of any ITP incident reports that were circulated since the previous meeting.

(2) A review of 2-3 of the Adjudicative Guidelines, with each ITWG member providing examples of how the guidelines might be reflected in reports from their area of responsibility.

(3) Overview of the UC Information Security program and relevant trends that could impact the ITP.

(4) Relevant training as determined by the ITPSO.

7. Training

a. ITPSO training requirements. The ITPSO will be required to comply with 32 CFR § 117.7(b)(4)(ii), including by taking the following courses to be completed within 90 days of their appointment to the position:

- Center for Development of Security Excellence (CDSE)'s *Insider Threat Program Management Personnel Curriculum INT 312.CU* *https://www.cdse.edu/Training/Curricula/INT312/* *(or an equivalent program)*

b. ITWG training requirements. All ITWG members will be required, prior to participation in the ITWG, to take, at a minimum, the CDSE's *Insider Threat Awareness Course # INT101.16* located at https://www.cdse.edu/Training/eLearning/INT101/

c. Training for all others involved in the ITP will be determined by the ITPSO, consistent with 32 CFR § 117.12(g).

8. Records UC CITP training and incident records will be maintained by the ITPSO on a confidential basis.

9. References

a. Executive Order 13526, "Classified National Security Information," December 29, 2009

b. 32 CFR part 117 ("NISPOM Rule")

c. REG 08.00.03 – Data Management Regulation

d. 32 CFR Part 147 Subpart A, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" as amended. ("Adjudicative Guidelines")