Standard Practice Guide Policies

Insider Threat Program

601.40

Applies to: All University-affiliated persons with authorized access to Federally-designated Sensitive Information, information systems, and associated research environments hosted, shared, or maintained by the University.

I. PURPOSE

The University of Michigan has legal, contractual, and ethical obligations to protect its sensitive research information, systems, research environments, and individuals with access to sensitive information. This policy implements U.S. Government requirements to protect Federally-designated sensitive research information. It establishes a holistic insider threat mitigation process that combines awareness and training with information security, physical security, and personnel assurance principles. The University of Michigan promotes and supports an institutional research culture that embraces an open and secure research environment by following these principles.

II. DEFINITIONS

A. Affected Information System: An information system owned, operated, or shared by U-M that receives, stores, generates, or transmits Federally-designated Sensitive Information.

B. Affected Person: A University-affiliated individual with authorized access to, or authority over, Federally-designated Sensitive Information, information systems, and associated research environments hosted, shared, or maintained by the University.

C. Affected Research Environment: A U-M physical location or logical access point (lab, office, enclave, cloud, or similar space) that receives, stores, generates, or transmits Federally-designated Sensitive Information.

D. Counterintelligence: The process of identifying, countering, neutralizing, and exploiting ongoing national security threats from foreign powers, organizations, and intelligence services and their associates to reduce the risk of espionage, economic espionage, insider threats, terrorism, and other threats to national security.

E. Federally-designated Sensitive Information: U.S. Government information (classified or unclassified) that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and Government-wide policies.

F. Insider: Any person with authorized access to a U-M resources (including personnel, facilities, information, equipment, networks, or systems) that has access to Federally-designated Sensitive Information.

G. Insider Threat: A person who uses their authorized access to U-M facilities, systems, equipment, information, or infrastructure to damage, disrupt operations, compromise information, or commit espionage or terrorists acts on behalf of a foreign entity.

H. Unauthorized Disclosure: A communication, confirmation, acknowledgement, or physical or electronic transfer of Federally-designated Sensitive Information, or making such information available in any way, to an unauthorized recipient.

III. POLICY

A. The U-M Insider Threat Program (ITP) implements a process to deter, detect, prevent, and mitigate or resolve behaviors and activities of trusted insiders that may present a witting or unwitting threat to Federally-designated Sensitive Information, information systems, research environments, and affected persons at U-M.

B. Principal Investigators, department chairs, deans of the schools and colleges, directors of the institutes and centers, and the Vice President for Research shall be responsible to support the provisions set forth in this SPG.

C. No University-affiliated person shall obstruct or impede any employee, hosted visitor, or contractor from reporting a contact, activity, indicator, or behavior relative to a potential insider threat.

D. Any University-affiliated person who intentionally reports a false or fabricated contact, activity, indicator, or behavior, which could compromise safeguarding of Federally-designated Sensitive Information, information systems, or research environments may be subject to appropriate corrective action.

E. It is a violation of Federal law and University policy to retaliate against a complainant for reporting, in good faith, potential insider threats, security incidents, or research misconduct.

F. A comprehensive ITP is essential to:

1. Deter affected persons from becoming insider threats;
2. Detect insider threats to Federally-designated Sensitive Information, information systems, research environments, and affected persons;
3. Prevent unauthorized disclosure or compromise of Federally-designated Sensitive Information, information systems, and research environments;

4. Mitigate potential insider threat risks to Federally-designated Sensitive Information, information systems, research environments, and affected persons, and;
5. Resolve actual insider threats to Federally-designated Sensitive Information, information systems, research environments, and affected persons.

IV. RESPONSIBILITY

A. The President of the University of Michigan and the U-M Facility Clearance Executive Committee (FCL-EC) exercise executive oversight of the U-M ITP.

1. The U-M President will appoint, in writing, an Insider Threat Program Senior Official (ITPSO) to manage the University's ITP in accordance with Federal laws, regulations, and Government-wide policies and guidelines.
2. At least annually, the U-M President will acknowledge, in writing to designated Federal agencies, the status of the U-M ITP and the University's support of the program.

B. The leaders of U-M Information Assurance, Human Resources, Office of General Counsel, Safety and Security, Provost, and Research programs will:

1. Collaborate with the ITPSO and an Insider Threat Program Working Group (ITPWG) to ensure affected persons, information systems, and research environments are adequately monitored to deter, detect, prevent, and mitigate or resolve insider threats.
2. Establish internal procedures to securely identify and refer relevant indicators of any potential or actual insider threats to the ITPSO and ITPWG in a timely manner.
3. Ensure access to such records and data as may be required by the ITPSO and ITPWG to perform authorized inquiries.

C. The ITPSO will:

1. Coordinate and implement, as needed, U-M policies and guidelines for successful deployment and maintenance of U-M's ITP.
2. Be responsible for day-to-day operations of the U-M ITP.
3. Establish an Insider Threat Program Working Group (ITPWG).
4. Develop insider threat awareness training, either in person or computer-based, to all affected persons granted access by the University to Federally-designated Sensitive Information, information systems, or research environments.
5. Ensure all affected persons receive adequate training and awareness of the requirements set forth in this policy.

6. Establish and promote an internal network site accessible to all affected persons to provide insider threat reference material, applicable reporting requirements and procedures, and a secure electronic means of reporting matters to the ITP.
7. At least annually, conduct a self-inspection of the U-M ITP, inform the U-M President and FCL-EC of the results, and outline projected resolutions to deficiencies, if any.
8. Ensure the ITPWG has timely access, as otherwise permitted, to available U.S. Government intelligence and counterintelligence reporting information and analytic products relative to insider threats, foreign intelligence services, and other adversarial threats.

D. The ITPWG will:

1. Serve as the U-M insider threat functional lead to assist with and coordinate insider threat and insider threat response activities with the ITPSO and immediately report potential or actual U-M insider threat activity to the ITPSO.
2. Assist the ITPSO to develop minimum standards and guidance to implement ITP policies, standards, and procedures.
3. Build and maintain a centrally managed insider threat analytic and response capability that manually and/or electronically gathers, integrates, reviews, assesses, and responds to insider threat information obtained through individual reporting venues, U-M administrative and academic offices, U-M monitored Federally-designated Sensitive Information system, and other sources as necessary and appropriate.
4. Establish procedures to securely request, receive, and retain records and documents necessary to complete assessments, inquiries, and resolutions required by this SPG.
5. Develop and implement procedures that ensure all ITP activities are conducted in accordance with applicable laws, whistleblower protections, and privacy policies.
6. Establish reporting guidelines for affected persons to refer relevant insider threat information directly to the ITPSO or ITPWG.
7. Assist the ITPSO to address common concerns (e.g., privacy and legal) and support the development of training, messaging to executives, managers, and the broader U-M population.
8. Serve as the U-M insider threat conduit to local, State, and Federal agencies and organizations.

E. Affected persons will:

1. Report to the appropriate U-M authority all contacts, activities, indicators, or behaviors they observe or gain knowledge of which could compromise safeguarding of Federally-designated Sensitive Information, information systems, or research environments.
2. Comply with the requirements of all current and applicable Federal laws, rules, regulations, and U-M policies concerning the responsible safeguarding of Federally-designated Sensitive Information, information systems, or research environments.

V. TRAINING

A. The ITPWG, and other U-M employees, as determined by the ITPSO, will receive and document the following initial and refresher training:
   1. Security and counterintelligence fundamentals;
   2. Indicators of insider threat behavior;
   3. Procedures to conduct insider threat inquiry and response actions;
   4. Laws and regulations regarding gathering, integration, retention, safeguarding, and use of Insider threat records and data;
   5. Applicable privacy laws, regulations and policies;

B. Affected persons will receive and document the following initial and refresher training:
   1. Relevant and potential threats to the U-M research and personal environment;
   2. Indicators of insider threat behavior;
   3. Importance of detecting insider threats by affected persons;
   4. Importance of reporting suspicious activity through appropriate channels;
   5. Methodologies of adversaries, including foreign intelligence entities, to recruit trusted insiders and collect Federally-designated Sensitive Information;
   6. Reporting requirements and procedures.

VI. REFERENCES

A. Executive Order 13556, Controlled Unclassified Information (November 2010).

B. 32 CFR Part 117, National Industrial Security Program (February 24, 2021).

C. 32 CFR Part 2002, Controlled Unclassified Information (September 14,2016).

D. Federal Information Security Modernization Act of 2014 (FISMA 2014).

E. Office of Management and Budget Circular A-130, Managing Federal Information as a Strategic Resource.

F. DoD Instruction 5200.48, Controlled Unclassified Information (2020-03-06).

G. Cybersecurity and Infrastructure Security Agency, Insider Threat Mitigation Guide (November 2020).

H. National Institute of Standards and Technology Special Publication 800-53r5, Security and Privacy Controls for Information Systems and Organizations.

I. National Institute of Standards and Technology Special Publication 800-171r2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

J. University of Michigan Standard Practice Guide 303.03, Policy Statement on the Integrity of Scholarship and Research.

K. University of Michigan Board of Regents Resolution Delegating Duties and Responsibilities Concerning Access To, Management, Handling, and Protection of Federally-Classified Information (May 16, 2019).

SPG Number:
601.40

Date Issued:
September 1, 2021

Last Updated:
September 1, 2021

Next Review Date:
September 1, 2026

Applies To:
All University-affiliated persons with authorized access to Federally-designated Sensitive Information, information systems, and associated research environments hosted, shared, or maintained by the University.

Owner:
Facility Clearance Executive Committee

Primary Contact:
Facility Security Officer (UMich.ITPSO@umich.edu)

Related Policies:
Background Screening (/policy/201.95)
Information Security (/policy/601.27)
Information Security Incident Reporting (/policy/601.25)
Institutional Data Resource Management Policy (/policy/601.12)
Privacy and the Need to Monitor and Access Records (/policy/601.11)
Responsible Use of Information Resources (/policy/601.07)
Security Clearance (/policy/201.53)
Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (/policy/601.33)
Violence in the University Community (/policy/601.18)
Weapon Possession (/policy/201.94)