# UTEP Insider Threat Program

## Introduction

The University of Texas at El Paso (UTEP) Insider Threat Program (ITP) aims to define insider threats unique to the University and to detect and identify those threats, assess their risk, and manage that risk before concerning behaviors manifest in an actual insider incident. The program will identify and protect critical assets (IP, research data and results, equipment, employees, etc.), prevent loss, and avert compromise of Federally Designated Sensitive Information (FDIS) [1].

The program will serve as a mechanism to encourage and incentivize correct behavior with training and awareness, policy and procedure, and management practices that guide employees to act in the interest and benefit of the University. Through this plan, we aim to understand the insider's interaction with UTEP systems and personnel, monitor that interaction as appropriate (leveraging technology and an incident response team as appropriate), and intervene to manage that interaction when it poses a threat. The ITP also addresses reporting and mitigation measures for cases where an insider threat incident is likely to or actually occurs.

## Authority

This ITP aligns with Regents Rules and Regulations, *Rule 10902*, Research Security Policies Sec. 2(b):

> Each U. T. institution shall appoint a Research Security Officer and establish a research security program that addresses key risk areas identified by federal and state governments, including National Security Presidential Memorandum-33 and Texas Education Code Section 51.956, which are applicable to each institution's research portfolio, including, but not limited to, intellectual property, cybersecurity, research and proprietary data security, clinical trial data security, foreign collaborations, foreign travel, foreign visitors, foreign scholars and scientists, insider threats, and any other key risk areas.

## Applies to

All University-affiliated individuals with authorized access to FDIS, information systems, and associated research data and environments hosted, shared, or maintained by the University [2].

---

[1] U.S. Government information (classified or controlled unclassified information) that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and Government-wide policies.

[2] Such individuals are referred to as Affected Persons or Affected Individuals in this ITP.

**Purpose**

The University of Texas at El Paso (UTEP) has legal, contractual, and ethical obligations to protect its research data (including sensitive information), systems, and research environments. 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 promotes and supports an institutional research culture that embraces an open and secure research environment by following these principles.

**Policy**

A. The ITP implements a process to deter, detect, prevent, and mitigate or resolve behaviors and activities of trusted insiders that may present an intentional or unintentional threat to critical University assets.

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

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. 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.

**Responsibilities**

A. The President of UTEP and Research & Innovation exercise executive oversight of the UTEP ITP.

1. The UTEP 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 UTEP President will acknowledge, in writing to designated Federal agencies, the status of the UTEP ITP and the University's support of the program.

3. The UTEP RSO will serve as interim ITPSO, until the official ITPSO is named.

B. The ITPSO will:

1. Coordinate and implement, as needed, policies and guidelines for successful deployment and maintenance of the ITP.

2. Be responsible for day-to-day operations of the ITP.

3. Establish an Insider Threat Program Working Group (ITPWG) consisting of Information Security, Information Resources, Human Resources, the Office of Legal Affairs, Environmental Health & Safety, Provost, and the Office for Research Protections.

4. Develop insider threat awareness training, leveraging existing training where appropriate, either in person or computer-based, and draft policy for training requirements for 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 ITP, inform the University President and Research & Innovation 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.

C. The ITPWG will:

1. Serve as the 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 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, administrative and academic offices, University 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 University population.

8. Serve as the UTEP insider threat conduit to local, State, and Federal agencies and organizations.

D. Affected persons will:

1. Report to the appropriate University 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 policies concerning the responsible safeguarding of Federally-designated Sensitive Information, information systems, or research environments.

**Training and Awareness**

The following training will be applied to individuals based on their role and type of access at the University.

A. The ITPWG, and other University 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 University 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 FDIS;
   6. Reporting requirements and procedures.

C. Other training specified by the ITPSO.

**References**


A. The University Of Texas at El Paso Information Security Incident Response Management Plan
B. UTEP Information Security Office Policies, Procedures, Standards, and Guidelines.
C. Executive Order 13556, Controlled Unclassified Information (November 4, 2010).
D. 32 CFR Part 117, National Industrial Security Program Operating Manual (December 21, 2020).
E. 32 CFR Part 2002, Controlled Unclassified Information (September 14, 2016).
F. Federal Information Security Modernization Act of 2014 (FISMA 2014).
G. Office of Management and Budget Circular A-130, Managing Federal Information as a Strategic Resource.
H. DoD Instruction 5200.48, Controlled Unclassified Information (2020-03-06).
I. Cybersecurity and Infrastructure Security Agency, Insider Threat Mitigation Guide (November 2020).
J. National Institute of Standards and Technology Special Publication 800-53r5, Security and Privacy Controls for Information Systems and Organizations.
K. National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, 800-171r2 and 800-171r3.

## Appendix A – Definitions

For the purposes of this Policy:

**Affected Information System**: An information system owned, operated, or shared by UTEP that receives, stores, generates, or transmits Federally Designated Sensitive Information (FDIS).

**Affected Person/Affected Individual**: 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.

**Affected Research Environment**: UTEP physical location or logical access point (lab, office, enclave, cloud, or similar space) that receives, stores, generates, or transmits FDIS.

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

**Insider**: Any person with authorized access to UTEP resources (including personnel, facilities, information, equipment, networks, or systems) that has access to FDIS.

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

**Unauthorized Disclosure**: A communication, confirmation, acknowledgement, or physical or electronic transfer of FDIS, or making such information available in any way, to an unauthorized recipient.