Policy 5.8: Insider Threat Policy

Volume: 1
Managing Office: Information Technology Services (ITS)/Office of Research Compliance (ORC)
Effective Date: June 15, 2024
Review History:
Authority: Information Technology Services/CIO

I. Purpose

Alabama A&M University (AAMU) 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. AAMU promotes and supports an institutional research culture that embraces an open and secure research environment by following these principles.

II. Definitions

For the purposes of this Policy:

A. **Affected Information System**: An information system owned, operated, or shared by AAMU that receives, stores, generates, or transmits Federally designated Sensitive Information.
B. **Affected Person**: 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**: AAMU 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 AAMU 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 AAMU 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. Scope

This policy encompasses all systems, automated and manual, for which the University has administrative responsibility, including systems managed or hosted by third parties on behalf of the entity. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

IV. Policy

A. The AAMU 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 AAMU.
B. Principal Investigators, Department Chairs, Deans of the Colleges, Director of Research Compliance, and the Vice President for Research and Economic Development shall be responsible to support the provisions set forth in this policy.
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.

V. Responsibilities

A. The AAMU CIO will exercise executive oversight of the AAMU ITP.

1. The AAMU CIO 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 AAMU CIO and/or ITP will acknowledge, in writing to designated Federal agencies, the status of the AAMU ITP and the University's support of the program.

B. The leaders of AAMU Information Technology Services, Human Resources, Office of General Counsel, Safety and Security, Provost, and Vice President for Research and Economic Development will:

1. Collaborate with the ITPSO 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 in a timely manner.
3. Ensure access to such records and data as may be required by the ITPSO to perform authorized inquiries.

C. The ITPSO will:

1. Serve as the AAMU insider threat functional lead to assist with and coordinate insider threat and insider threat response activities with the CIO/Information Technology Services and immediately report potential or actual AAMU insider threat activity to the President and appropriate authorities.
2. Coordinate and implement, as needed, AAMU policies and guidelines for successful deployment and maintenance of AAMU's ITP.
3. Be responsible for day-to-day operations of the AAMU ITP.

4. Establish an Insider Threat Program Working Group (ITPWG).
5. 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.
6. Ensure all affected persons receive adequate training and awareness of the requirements set forth in this policy.
7. 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.
8. At least annually, conduct a self-inspection of the AAMU ITP, inform the AAMU President of the results, and outline projected resolutions to deficiencies, if any.
9. 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.
10. Serve as the AAMU insider threat conduit to local, State, and Federal agencies and organizations.

D. The ITPWG will:

1. Assist the ITPSO to develop minimum standards and guidance to implement ITP policies, standards, and procedures.
2. Establish procedures to centrally manage an insider threat capability to monitor for and respond to indicators of an insider threat.
3. Establish procedures to securely request, receive, and retain records and documents necessary to complete assessments, inquiries, and resolutions required by this policy.
4. Develop and implement procedures that ensure all ITP activities are conducted in accordance with applicable laws, whistleblower protections, and privacy policies.
5. Establish reporting guidelines for affected persons to refer relevant insider threat information directly to the ITPSO or ITPWG.
6. 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 AAMU population.

E. Affected persons will:

1. Report to the appropriate AAMU 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 AAMU policies concerning the responsible

safeguarding of Federally designated Sensitive Information, information systems, or research environments.

VI. Training

A. The ITPWG, and other AAMU 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 AAMU 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.

VII. Compliance

Failure to comply with this Policy and/or regulations promulgated hereunder will be deemed a violation of University Policy and subject to disciplinary action in accordance with the disciplinary guidelines as outlined in the Faculty or Staff Handbook, whichever one is applicable to the individual.

VIII. Revision History

- June 2024 Policy Updated (DRAFT)

IX. Authority: President

X. Responsible Office: President/Chief Information Officer

XI. Related Documents

- University Policy 5.7: Data, Information Access, and Security Policy

XII. 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.