Policy 5.8

Volume
Managing Office

Effective Date
Review History:
Authority

I. Purpose

Alabama A&M University (AAMU) has legal, contractual, and ethical obligations to protect its sensitive research information, systems, research environments, and

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. Mh7c85plosur threats s(a)4(r)-7(c)4(h e)4(nvi)-2(r)3(onm)-26z6Tc amo 0 Tc 0o> 4c8

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.