15.05 System Research Security Office

Approved February 6, 2020 (MO -2020)
Next Scheduled Review: February 6, 2025

Policy Summary

The Board of Regents (board) of The Texas A&M University System (system) is committed to the highest standards of integrity and compliance in ensuring the security of its member's research portfolios. This policy establishes the framework for (a) designating the system Research Security Office (RSO) as the responsible office for classified information, controlled unclassified information, management of the system's secure computing enclave, foreign influence reporting, and export controls, (b) achieving the highest level of compliance with applicable ethical, legal, regulatory, contractual and system standards and requirements in securing research portfolios, (c) promoting an organizational culture of compliance in meeting federal requirements to maintain federal funding, and (d) assisting members in related compliance operations.

Policy

1. SYSTEM RESEARCH SECURITY OFFICE

The vice chancellor for research appoints a chief research security officer (CRSO) who, through the Office of Research, has access to the chancellor and administers the functions of the RSO, including research security policies, procedures and technology to enable members to comply with federal guidelines for handling all levels of U.S. government information. The RSO works closely with the Office of General Counsel and the System Ethics and Compliance Office, as needed.

1.1 Specifically, the RSO serves as the responsible office for:

(a) classified information programs;

(b) controlled unclassified information programs;

(c) management of the system's secure computing enclave;

(d) foreign influence reporting programs; and

(e) export control programs.

1.2 In support of these programs and to promote a culture of compliance, the RSO undertakes the following activities:

(a) develop, implement, and monitor a system-wide research security compliance program (For the purposes of this policy, a system-wide research security compliance program refers to administration of the classified, controlled

unclassified, secure computing enclave, and foreign influence reporting programs; and administrative oversight of export control programs designed to ensure each member developments, implements, and maintains an appropriate export control program, and to facilitate export control compliance programs within and between members.);

(b) advise and assist members in related compliance activities to include but not limited to developing related best practices;

(c) provide educational opportunities for members, such as the system export control affinity group;

(d) coordinate with member empowered officials prior to their contact with federal regulatory agencies when instances of related known or suspected non-compliance occur; and

(e) collaborate with members to develop appropriate related risk mitigation strategies.

1.3 Additionally, the RSO serves as the system's federal interface with regards to the following operating procedures:

(a) the system facility security officer and the insider threat program senior official as required by the *National Industrial Security Program Operating Manual*;

(b) focal point for communications with the federal intelligence community;

(c) point of contact for ensuring compliance with all aspects of the U.S. Department of Defense Cyber Maturity Model; and

(d) point of contact for communicating with federal agencies in regards to counter intelligence issues.

2. SHARED SERVICES

2.1 As a shared service entity, members work closely with the RSO in exercising the office's available resources (subject matter expertise, equipment, training, etc.).

2.2 The RSO advises and assists members through outreach networks established with member stakeholders.

Related Statutes, Policies, or Requirements

System Policy *15.02, Export Controls Program Management*

System Regulation *15.05.01, Classified Information Management*

System Regulation *15.05.02, Controlled Unclassified Information Management*

System Regulation *15.05.03, Secure Computing Enclave Management*

Member Rule Requirements

A rule is not required to supplement this policy.

Contact Office

System Research Security Office
(979) 862-1965