

## 15.05 System Research Security Office



Revised [February 9, 2023](#) (MO -2023)  
Next Scheduled Review: February 9, 2028  
Click to view [Revision History](#).

---

### 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 control program management, (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 System Office of General Counsel (OGC), the System Office of Information Technology (OIT), and the System Ethics and Compliance Office (SECO), 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.
- (e) Export control program management.
- (f) Coordination of National Security Presidential Memorandum (NSPM) 33 requirements.

- 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 systemwide research security compliance program (For this policy, a systemwide research security compliance program refers to the administration of the classified, controlled unclassified, secure computing enclave, and foreign influence reporting programs; administrative oversight of export control program management designed to ensure each member develops, 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, including 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 before their contact with federal regulatory agencies when instances of related known or suspected non-compliance occur.
  - (e) Collaborate with members to develop appropriate related risk mitigation strategies.
- 1.3 Additionally, the RSO serves as the system's federal interface regarding the following operational 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) The focal point for communications with the federal intelligence and enforcement communities.
  - (c) Point of contact for ensuring compliance with all aspects of the U.S. Department of Defense Cyber Maturity Model Certification.
  - (d) Point of contact for ensuring compliance with all aspects of NSPM-33, including, but not limited to, required certifications and research security program implementation.
  - (e) Point of contact for communicating with federal agencies regarding counterintelligence 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 15.05.04, High Risk Global Engagements and High Risk International Collaborations](#)

---

## **Member Rule Requirements**

---

A rule is not required to supplement this policy.

---

## **Contact Office**

---

Research Security  
(979) 862-1965