15.05.02 Controlled Unclassified Information Management

Revised February 16, 2023
Next Scheduled Review: February 16, 2028
Click to view Revision History.

Regulation Summary

The Texas A&M University System (system) is required to comply with information protection standards outlined by the U.S. Information Security Oversight Office (ISOO) for safeguarding controlled unclassified information (CUI), subsequently stored in the system's nonfederal information systems according to 32 CFR 2002. This regulation establishes requirements and procedures in meeting federal requirements for securing CUI.

Regulation

1. SECURITY PROCEDURES

1.1 The vice chancellor for research appoints a chief research security officer (CRSO) who oversees the system's CUI program. While the system Research Security Office (RSO) is responsible for implementing the CUI program, members must work closely with the RSO to promote a culture of compliance.

1.2 In consultation with appropriate system or member offices, the system RSO defines, establishes, and authorizes information security standards and systems to comply with the requirements of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. The system RSO manages and maintains the secure computing enclave (SCE) and other secure computing resources, which collectively are systemwide information technology resources that all members use to secure federally regulated CUI.

(a) Under System Policy *15.05, System Research Security Office*, the system RSO serves as the point of contact for ensuring compliance with all aspects of the U.S. Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC).

(b) The system RSO serves as the authorizing official for any system.

The system RSO reviews, assesses, and validates all system-established SCEs proposed by members for compliance with the NIST SP 800-171 requirements.

1.3 The Defense Counterintelligence and Security Agency (DCSA) maintains CUI oversight on behalf of the Department of Defense. The system RSO will conduct periodic self-inspections as appropriate to ensure continued compliance with the CUI requirements.

2. INDIVIDUAL RESPONSIBILITY

2.1 Employees with access to CUI must ensure such information is protected according to applicable U.S. Government and contractual requirements.

2.2 Employees with access to CUI must ensure that information is only disclosed to persons who are authorized to have access and who also have a need to know.

2.3 Employees with access to CUI must complete TrainTraq Course #2113511 once every two years and any other course as determined by the CRSO.

3. SECURITY PROCEDURE VIOLATIONS

3.1 Violations of security procedures must be immediately reported to the CRSO. Examples of security violations include, but are not limited to:

(a) Allowing unauthorized individuals to have access to CUI.

(b) Transmitting or processing CUI without encryption.

(c) Removing CUI from the facility, where it is usually stored, without permission.

(d) Copying or destroying CUI using unapproved resources.

(e) Generating or processing CUI outside of appropriately secured devices.

3.2 Substantiated violations can lead to disciplinary action up to and including dismissal.

Related Statutes, Policies, or Requirements

Exec. Order No. 13556, 75 Fed. Reg. No. 216 (Nov. 9, 2010).

32 CFR 2002, Information Security Oversight Office, National Archives

System Policy *15.05, System Research Security Office*

Controlled Unclassified Information (CUI) Marking Handbook

Protecting CUI in Nonfederal Information Systems and Organizations

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

Research Security
(979) 862-1965