15.05.02 Controlled Unclassified Information Management

Approved February 10, 2020
Next Scheduled Review: February 10, 2025

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 pursuant to 32 CFR 2000. This regulation establishes requirements and procedures in meeting federal requirements for securing CUI.

Regulation

1. SYSTEM RESEARCH SECURITY OFFICE

1.1 The vice chancellor for research will appoint a chief research security officer (CRSO) who is responsible for overseeing the protection, marking and dissemination, and destruction of CUI.

1.2 The system Research Security Office (RSO) manages and maintains the secure computing enclave (SCE) which is a systemwide information technology resource that is used by all members to secure federal information, including but not limited to CUI. Procedures related to the management of the SCE are contained in System Regulation *15.05.03, Secure Computing Enclave Management*.

1.3 While the RSO is responsible for implementing CUI compliance, members must work closely with the RSO in promoting a culture of compliance.

1.4 CUI must be stored in and processed from the SCE. In the event an exemption is requested and subsequently granted pursuant to Section 1.5, controlled portions of information must be encrypted to protect them from theft. Local information systems used to process or store CUI must comply with NIST SP 800-171 *Protecting CUI in Nonfederal Systems*, and must only be utilized in the event an exemption from use of the SCE is both requested and granted from the CRSO.

1.5 To request exemption from use of the SCE, when required pursuant to Section 1.4, a formal request must be submitted to the CRSO. The CRSO will have final authority in granting the exemption, requiring certain security measures be implemented as conditions of granting the exemption, or denying the exemption request. If an exemption is granted, the project and related information systems will be subject to continuous follow-up and internal auditing by the CRSO to ensure related federal and system standards are being met.

1.6 On a project basis and in coordination with affected members, when a research project terminates, the CRSO will develop CUI cleanup and destruction procedures for controlled data in the SCE and any controlled data maintained outside of the SCE (e.g., data on mobile devices or physical documents).

1.7 Detailed formal documentation of the specific process related to the management of CUI is contained in the RSO CUI internal manual.

2. INDIVIDUAL RESPONSIBILITY

2.1 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.

2.2 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 dissemination-controlled CUI;

(b) transmitting CUI without encryption;

(c) removing CUI from the facility, where it is normally stored, without permission;

(d) copying or destroying CUI using unapproved resources; or

(e) generating or processing CUI outside of the SCE without authorization from the CRSO or designee.

3.2 When those responsible for a procedural violation can be determined and one or more of the following factors are evident, a report will be submitted to the responsible federal agency.

(a) Deliberate disregard of CUI security requirements;

(b) Gross negligence in the handling of CUI material; or

(c) A pattern of negligence or carelessness exists.

3.3 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 2000, Information Security Oversight Office, National Archives

System Policy *15.02, Export Controls Program Management*

System Policy *15.05, System Research Security Office*

System Regulation *15.05.03, Secure Computing Enclave Management*

Controlled Unclassified Information (CUI) Marking Handbook

Protecting CUI in Nonfederal Systems and Organizations

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

System Chief Research Security Officer
(979) 862-1965