FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Protection of Controlled Unclassified Information (CUI) #1930.001

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
March 3, 2025	March 3, 2025	Division of Information Technology Information Security

POLICY STATEMENT

Florida International University is committed to executing its operations and research mission in a secure and consistent manner in accordance with relevant laws and regulations. Specifically, the University requires compliance with all applicable cybersecurity standards prescribed by federal, state, institutional regulations as well as the government-wide online repository for federal-level guidance regarding Controlled Unclassified Information (CUI) and applicable grant and contract terms and conditions.

SCOPE

This policy applies to all offices, academic, and operational departments at all Florida International University locations, owned and leased, that access or engage with Controlled Unclassified Information (CUI). It also applies to all FIU faculty, staff, students, affiliates, partners, visitors, contractors and subcontractors (and their employees and agents) who access, work with, store, and transmit CUI data and applications or otherwise engage with CUI.

REASON FOR POLICY

Controlled Unclassified Information refers to data that, while not classified, is still sensitive and requires safeguarding or dissemination controls in accordance with federal regulations and guidelines. . In connection with some of its activities, operations, and sponsored research projects, the University may receive or create Controlled Unclassified Information ("CUI"), which requires compliance with safeguards and/or dissemination controls. This policy sets forth the requirements, expectations, and guidance for CUI compliance. It applies to all CUI handlers, as defined below, including faculty, staff, students and affiliates or agents who, on behalf of the university, may use, create, or process CUI in any way, including marking, safeguarding, transporting, disseminating, re-using, or disposing of the information.

DEFINITIONS

TERM	DEFINITIONS
Controlled Unclassified Information (CUI)	Refers to information defined by federal regulation, 32 C.F.R. § 2002.4(h), and by Presidential Executive Order 13556 as information that the U.S government creates or possesses, or that an entity creates or possess for or on behalf of the federal government, that a law, regulation, or Federal Government–wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.
CUI Handlers	Means any faculty, staff or students, who may handle, possess, use, share, create, or receive CUI, and includes any affiliates, contractors, or agents of the university who may need to be given access to or engage with CUI on behalf of the university or in connection with university research projects.
CUI Registry	Refers to the Government-wide online repository for Federal-level guidance regarding CUI policy and practice maintained by The National Archives and Records Administration (NARA). The NARA provided a CUI Registry List which includes multiple categories and subcategories, some of which will overlap with export control regulations, as follows: : 1. Controlled Defense Information (CDI): Controlled Defense Information is a category of CUI. CDI is a specific term used by the DoD to describe information that requires safeguarding under the DFARS Clause 252.204-7012; it is defined as: • Controlled Technical Information (CTI) • DoD Critical Infrastructure Security Information • Naval Nuclear Propulsion Information • Unclassified Controlled Nuclear Information (UCNI) – Defense 2. Export Control Information: Also a category of CUI, this refers to unclassified information concerning certain commodities, materials, technology, software ("items"), or other information whose export could reasonably be

	expected to adversely affect the United States national security and nonproliferation objectives. This includes "dual use" items as they appear on the Commerce Control List in the Export Administration Regulations (EAR); defense articles that fall under the International Traffic in Arms Regulations' US Munitions List (ITAR); and certain sensitive nuclear technology governed under the Department of Energy's Export Regulations. There are other categories of CUI that are common in a university setting and which also require safeguarding, for example: Patent, Privacy, Financial, International Agreements, Immigration, Procurements & Acquisition.
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 (NIST SP 800-171)	Outlines the guidelines and requirements for "Protecting Controlled Unclassified Information CUI in Nonfederal Systems and Organizations." The requirements apply to all components of nonfederal information systems and organizations that process, store, transmit CUI, or provide security protection for such components.
Cybersecurity Maturity Model Certification (CMMC)	Cybersecurity Maturity Model Certification (CMMC) The CMMC is a program established by the United States Department of Defense (DoD) to standardize security practices and processes intended to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
CMMC Enclave	Highly Secured environment where CUI should be stored.
Managed Service Provider	An organization responsible for managing and delivering services to another organization as per their requirement for CMMC.

ROLES AND RESPONSIBILITIES

Federal Agencies: Federal agencies are responsible for determining when CUI will be exchanged or potentially created as part of an award or other transaction. CUI requirements are defined as a term and condition within an agreement along with corresponding cybersecurity measures to protect the CUI. As federal agencies continue to implement CUI requirements in agreements, the implementation of specific cybersecurity measures may differ. Federal agencies can develop and promulgate their own general purpose or project-specific clauses to specify safeguarding requirements for information or information systems.

Principal Investigator (PI): PIs are responsible for understanding and identifying research projects involving CUI as soon as possible so that proper steps can be taken to evaluate and

negotiate acceptable terms and conditions. As part of this process, PIs should consider alternatives to using or generating CUI whenever possible due to the high level of protection required for projects that generate or receive CUI. It is vital to properly protect CUI whenever the University agrees to accept a project that includes the receipt or generation of CUI. Typically, this process is supported by FIU''s Export Control team in coordination with ORED's IT Security Specialist who work with the PI and research team to create the appropriate Technology Control Plan (TCP) and System Security Plan (SSP) to address export control and data security requirements. As specified in this compliance documentation, PIs are responsible for monitoring CUI compliance within their sponsored projects, which includes oversight of trainees, staff, collaborators, and subawardees.
Consequences for not protecting CUI include:

- Loss of data and/or vulnerability to research security breaches and unauthorized data access
- Loss of research funding by federal and state agencies
- Cost and liability of contractual breach of contract
-
- Significant monetary fines and penalties resulting from federal enforcement
- Reputational risk for FIU and PIs that adversely impacts FIU's research opportunities. Office of Research and Development (ORED): works together with the PI and their department and college to submit and negotiate all sponsored projects and research related non-financial agreements that may require the receipt or generation of CUI.

Division of Information Technology: provides helpful IT resources to FIU faculty in support of their teaching, research, and daily work. DoIT IT Security Office works collaboratively with ORED and the PI whenever there are specific cybersecurity provisions in sponsored project awards. In cases where CUI will be received or generated under a financial or non-financial agreement, PI's are required to use FIU's CMMC Enclave.

Office of Compliance and Integrity: Coordinates closely with ORED's Sponsored Research team to proactively identify export control requirements associated with data security requirements; coordinate the appropriate compliance solution and documentation with the PI; and ensure that the PI/research team is fully trained on these joint export control and CUI requirements. Where appropriate, University Compliance/Export Control will advise ORED's contract negotiating team on removing export and data security restrictions through negotiated sponsor agreement terms. With respect to international travel approvals (Travel Authorization Requests), University Compliance/Export Control also flags IT security requirements intended to support the traveler while abroad, including special "clean lap-top" provisioning for approved travel to Foreign Countries of Concern (FCCs).

RELATED RESOURCES

FIU Security | Cybersecurity Maturity Model Certification (CMMC)
FIU Cybersecurity Maturity Model Policy Library
Protection of CUI Procedure

CONTACTS

IT Security Office | 305-348-1366
Office of Research and Development |

HISTORY

Initial Effective Date: March 3, 2025
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): March 3, 2025.