



FIU CUI Acceptable Use Policy

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
08/04/2025	09/26/2025	Division of Information Technology

POLICY STATEMENT

Florida International University (FIU) users should be aware that all equipment that is FIU-owned, department owned, grant owned, network infrastructure, FIU CUI cloud-based enclave, FIU-ARC CUI infrastructure, FIU data, research data and software applications are the property of FIU and are to be used for official use only.

All data residing on FIU-owned equipment is the property of FIU and therefore should be treated as such and protected from unauthorized access.

SCOPE

This policy applies to:

- All authorized users (employees, students, contractors, partners, and third parties)
- All access to the CUI Enclave and ARC CUI
- All systems, networks, and information (including CUI) processed, stored, or transmitted via the CUI Enclave and ARC CUI

REASON FOR POLICY

The purpose of this Acceptable Use Policy (AUP) is to outline the acceptable and unacceptable use of the FIU CMMC enclave (CUI Enclave) environment and the FIU-ARC CUI Lab (ARC CUI), which are configured to handle Controlled Unclassified Information (CUI) in accordance with applicable laws, regulations, and contractual requirements.

This policy ensures protection of CUI, system integrity, and compliance with NIST SP 800-171, DFARS 252.204-7012, CMMC Level 2 requirements, and other applicable federal standards.



Acceptable Use

Authorized users **must**:

- Access the CUI Enclave and ARC CUI environments only for official business-related purposes
- Authenticate using **multi-factor authentication (MFA)** and comply with strong password policies
- Secure all passwords used to access CUI Enclave and ARC CUI environments and be kept secure and protected from unauthorized use
- Never share user accounts between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- Never forward emails containing CUI received on the FIU CUI Office 365 Government tenant to FIU email account or personal account
- Use extreme caution when opening e-mail attachments received from unknown senders
- Only perform off-campus work connected to the secure FIU VPN connection
- Ensure that **CUI is only accessed, processed, or transmitted** within the secure FIU Enclave and/or ARC CUI environments
- Log off or lock the session when not actively using the Virtual Desktop Infrastructure (VDI)
- Report **security incidents or suspicious activities immediately** to the IT Security team
- Store all sensitive or regulated data **only** within the VDI environment and **not** on local or unauthorized cloud storage
- Participate in **annual CUI/CMMC and annual FIU Cybersecurity Awareness training**
- Properly label CUI data using the appropriate sensitivity label
- Encrypt CUI in emails and web transactions using authorized methods

Prohibited Activities

Users **must not**:

- Use CUI for personal financial gain or engage in political activities
- Download or view offensive, defamatory, obscene, or racist materials
- Attempt to disable or circumvent security controls (e.g., DLP, AV, logging, monitoring)
- Download, copy, or move CUI outside of the CUI Enclave or ARC CUI environments
- Access or share CUI with unauthorized individuals or systems
- Share CUI-related information in GenAI tools
- Use the CUI Enclave or ARC CUI environments for personal activities (e.g., social media, personal email, shopping)
- Install or use unauthorized software or browser extensions within the VDI
- Use weak, reused, or shared passwords
- Use public or unsecured networks without VPN or secure tunneling



Data Protection & Privacy

- All data within the VDI is subject to **monitoring and logging** for security and compliance purposes
- Users should have **no expectation of privacy** for actions performed within the CUI Enclave or ARC CUI environments
- Transmission of CUI must follow **FIPS 140-2 validated encryption** standards

Compliance and Enforcement

- Violation of this policy may result in:
- Revocation of access
- Disciplinary action
- Legal action if applicable under federal law or contractual obligations
- Regular audits and monitoring will be conducted to ensure adherence to this policy
- Report offensive messages, security issues or suspected violations to the FIU IT Security Office immediately at security@fiu.edu

Policy Review

This policy will be reviewed at least annually or whenever there are significant changes to regulations, environment architecture, or the threat landscape.

DEFINITIONS

TERM	DEFINITIONS
ARC	Applied Research Center
Cybersecurity Maturity Model Certification (CMMC)	CMMC is a U.S. Department of Defense program that standardizes cybersecurity practices to protect sensitive unclassified information, including Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). CMMC compliance is tied to NIST SP 800-171, Federal Acquisition Regulation (FAR) Clause 52.204-21, and Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012.
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.

ROLES AND RESPONSIBILITIES

Each member of the University community utilizing the CUI Enclave and/or ARC CUI Lab is responsible for adhering to all federal, state and local laws and FIU rules, regulations and policies, as the same may be amended from time to time, pertaining to the security and protection of electronic information resources that he/she uses, and/or over which he/she has access or control.

Persons who fail to adhere to this Policy may be subject to penalties as provided by law and/or disciplinary action, including dismissal or expulsion. Violations will be handled through the University disciplinary policies applicable to employees and students. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Unauthorized or fraudulent use of university computing or telecommunications resources can also result in felony prosecution as provided for in the Federal and State of Florida Statutes.

RELATED RESOURCES

Policy: Protection of Controlled Unclassified Information (CUI) 1930.001 - <https://policies.fiu.edu/files/953.pdf>

More information about CMMC at FIU can be found at <https://security.fiu.edu/governance/cmmc/>

CONTACTS

*Division of Information Technology
Information Technology Security Office - PC534
11200 SW 8 ST, Miami, FL 33199
305-348-1366*



FLORIDA
INTERNATIONAL
UNIVERSITY



HISTORY

Initial Effective Date: August 4, 2025

Review Dates (review performed, no updates): 9/26/2025

Revision Dates (updates made to document): 9/26/2025