FIU & ARC
CUI Acceptable Use Policy

8/04/2025

DOCUMENT CHANGE HISTORY
The table below identifies all changes that have been incorporated into this document.

Change	Date	Version	Change Description
Document Creation	8/13/2025	1	Document Created
Review	9/26/2025	1	Policy Reviewed, no changes
Formatting	2/3/2026	1	Updated formatting to match other CMMC policies

Table of Contents

1.0 Overview

1.1 Background

Florida International University and the Applied Research Center (FIU & ARC) must implement policies for its electronic information systems that maintain organizational information. These policies shall ensure access only to those workforce members and software applications that have been authorized access.

1.2 Purpose

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.

1.3 Scope

This policy applies to:

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

1.4 Roles

Chief Information Security Officer (CISO): The CISO's role is to oversee the organization's access control strategy to ensure the confidentiality, integrity, and availability of information systems, including those handling Controlled Unclassified Information (CUI). The CISO ensures that access control policies align with CMMC requirements and other relevant security frameworks, working closely with System Administrators, Human Resources, and department heads to enforce proper access management practices across the institution.

Office of Research and Economic Development (ORED): The Office of Research and Economic Development (ORED) plays a key role in ensuring that research activities involving Controlled Unclassified Information (CUI) comply with access control requirements under CMMC. ORED collaborates with System Administrators and the Information Technology Security Office (ITSO) to ensure that researchers, staff, and external partners are granted appropriate access to CUI-related systems and facilities in accordance with institutional policies and regulatory requirements.

External Service Provider (ESP): The External Service Provider (ESP) is responsible for managing user accounts, access controls, and system permissions for individuals handling Controlled Unclassified Information (CUI). As a key security partner, the ESP ensures that access to CUI-related systems, including Office 365 and other institutional platforms, is properly

configured, maintained, and monitored in compliance with CMMC requirements and institutional policies.

Applied Research Center (ARC): The Applied Research Center provides an effective and responsive interface between Florida International University and government and commercial sectors via their on premises network. The ARC has its own staff of administrators responsible for managing user accounts, access controls, and system permissions for individuals handling Controlled Unclassified Information (CUI).

1.5 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.

Chief Information Security Officer (CISO): The CISO is responsible for developing and enforcing the Access Control Policy to ensure compliance with CMMC requirements. They oversee access management processes, conduct regular audits, and work with System Administrators and Human Resources to manage user provisioning, modifications, and terminations. The CISO is responsible for ensuring access control incidents are investigated, appropriate corrective actions are taken, and the institution remains prepared for compliance assessments.

Office of Research and Economic Development (ORED): ORED is responsible for determining which users require access to CUI and defining the level of access needed based on their roles and research responsibilities. They work closely with the CISO and ITSO to facilitate proper access provisioning, ensuring compliance with access control policies. ORED reviews and approves access requests, maintains documentation for compliance purposes, and supports periodic audits to verify proper access management. Additionally, they integrate access control requirements into research agreements and sponsored project contracts to align with federal regulations and institutional security policies.

External Service Provider (ESP): The ESP is responsible for provisioning, modifying, and revoking user access to CUI-related systems based on approvals from ORED and institutional security teams. They enforce access control policies by implementing role-based access controls,

multi-factor authentication (MFA), and least-privilege principles. The ESP continuously monitors system access for unauthorized activity, conducts periodic access reviews, and provides audit logs to the institution for compliance verification. They also ensure that access management practices align with institutional policies and regulatory requirements, assisting with security assessments and incident response efforts related to access control.

Applied Research Center (ARC): The ARC is responsible for provisioning, modifying, and revoking user access to CUI-related systems. They enforce access control policies by implementing role-based access controls, multi-factor authentication (MFA), and continuously monitors system access for unauthorized activity via audit logs for compliance verification.

1.6 Definitions

ARC - Applied Research Center

Cybersecurity Maturity Model Certification (CMMC) - 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.

1.7 Management Statement

The items contained in this document are required of all FIU & ARC users regardless of role within the organization. Failure to abide by the items defined in this document pose a risk to the organization in the event of breach or audit. Any non-conformance to this document may result in the disciplinary provisions being exercised.

1.8 Regulatory References

- NIST 800-171r2
- NIST 800-53 rev. 5
- CMMC 2.0
- 45 CFR: 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(1), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(C),

164.312(a)(2)(i), 164.312(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(2)(iv), 164.308(a)(4)(ii)(A), 164.312(a)(2)(iii), 164.308(a)(5)(ii)(C)

2.0 Policy

Access Control 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.

Acceptable use

Authorized use is defined as:

Access Scope

- Users are authorized to access the FIU CUI Enclave and ARC CUI Environment for official, business- or contract-related purposes involving CUI.

Authentication and Account Security

- Users must authenticate using multi-factor authentication (MFA).
- Users must use strong passwords in accordance with FIU policies and maintain their confidentiality.
- Users are responsible for the security of their accounts and credentials.

Email Handling and Communication

- Users are authorized to send, receive, and review CUI emails within the FIU CUI Office 365 Government tenant using approved encryption methods.
- Users are authorized to open and review email attachments from trusted sources within the secure tenant.

Data Storage and Processing

- Users are authorized to store CUI in approved systems within the FIU CUI Enclave and ARC CUI Environment.
- Users are authorized to apply approved sensitivity labels to CUI documents and data.
- Users are authorized to process, edit, and collaborate on CUI only within the secure enclave and environment.
- Users are authorized to access and utilize Microsoft O365 services in the GCC-H tenant.
- Users are authorized to access government websites such as DoD safe to access and download CUI content.

Remote / Off-Campus Work

- Users are authorized to access CUI resources off campus as long as appropriate safeguards are implemented. For example, the use of privacy screens, working in a private location, and logging out of accounts when stepping away from the computer.

Virtual Desktop Infrastructure (VDI) Use

- Users are authorized and required to lock or log off VDI sessions when not actively using them.
- Users are authorized and required to close browser windows or VDI sessions containing CUI when leaving devices unattended.

Monitoring and Accountability

- Users' activities within the FIU CUI Enclave and ARC CUI Environment are logged and monitored for compliance.
- Users are authorized and required to report security incidents or suspicious activity immediately to the IT Security team.

Training and Awareness

- Users are authorized and required to participate in annual CUI/CMMC and FIU Cybersecurity Awareness training, including training specific to proper handling of CUI within O365, the FIU CUI Enclave, and ARC CUI Environment.

Detection and Monitoring Mechanisms

- Authorized access and actions are audited and logged to ensure compliance.
- Users' approved CUI sharing, labeling, and encryption actions are verified through system monitoring tools.
- Users' engagement in training and awareness programs is tracked to confirm ongoing eligibility for authorized access.
- All activity and instances of authorized or unauthorized use of the system are captured in Sentinel audit logs. Automated alerts are generated based on malicious or unauthorized activity.

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

3.0 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

4.0 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

Approval

Upon review of this document, all signatories below acknowledge their approval of the information indicated within this document. Signature indicates information is agreed upon by all parties. Any updates to this document will require subsequent approvals by the below individuals and/or their designees in the event the identified individuals are unavailable.

Signed by:
Helvetiella Longoria
38216B0029734A8...

2/12/2026

Chief Information Security Officer | Date