



UNIVERSITY OF CENTRAL FLORIDA

Office of the President

SUBJECT: Controlled Unclassified Information Policy	Effective Date: 5/2/2023	Policy Number: 4-217
	Supersedes:	Page Of 1 10
	Responsible Authority: Director, Office of Cyber Risk Management	

APPLICABILITY/ACCOUNTABILITY

This policy applies to all members of the university community who handle and protect Controlled Unclassified Information (CUI) on behalf of the University of Central Florida (UCF).

BACKGROUND

CUI is information the government creates or possesses, or an entity (such as UCF) creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires safeguarding or dissemination controls. The loss or improper safeguarding of CUI can directly impact national security and thus [Presidential Executive Order 13556](#) requires standardized protections across *all* systems (federal and non-federal) handling CUI. Federal regulations at [32 CFR Part 2002](#) implement the federal CUI Program and includes specifications to identify, mark, access, disseminate, safeguard, decontrol, and destroy CUI and the requisite standards by the National Institute of Standards and Technology (NIST) that applies.

UCF primarily encounters CUI through sponsored research or other university activities with a federal agency. The requirement to safeguard CUI received or generated by UCF can flow down from the federal government directly or indirectly through a contract or a nondisclosure or data use agreement. As a condition of acceptance, UCF must comply with the agreement terms, which may include operational requirements beyond the applicable NIST standard.

UCF developed the secure enclave known as Knight Shield to meet federal CUI security requirements and reduce the compliance burden on researchers. The core operations of Knight Shield are funded by the university, with unique needs to be addressed by each respective research project. Knight Shield is registered with the federal government, as required for non-federal information systems handling CUI on behalf of the Department of Defense (DoD).

POLICY STATEMENT

The University of Central Florida is committed to compliance with federal cybersecurity protections for CUI. The Office of the Chief Information Officer (CIO) is responsible for the oversight of information technology and information security solutions. The Office of the Chief Information Security Officer (CISO) is responsible for the university's information security. The Office of Research (OR) is the designated authority for sponsored program activities. The Office of Cyber Risk Management (OCRM) oversees cybersecurity compliance, recordkeeping, and implementation of the business processes and accountability to safeguard CUI across the research enterprise.

Knight Shield is designated by OR as the approved environment to electronically store, process, or transmit CUI for sponsored research agreements. Alternative environments may only be utilized after written approval is obtained from OCRM in coordination with the CISO.

Individuals acting on behalf of the university who handle CUI related to sponsored research *or* operate a controlled environment or device that safeguards CUI are responsible for adhering to the policies, standards, and procedures issued by OCRM. These requirements include **background checks and screening, training, and ensuring CUI is properly marked, stored, accessed, disseminated, safeguarded, decontrolled, and destroyed** according to the laws, regulations, and standards governing CUI.

Security incidents are to be reported to the Security Incident Response Team at SIRT@ucf.edu, as defined by policy 4-008, *University Data Classification and Protection Policy*. When the suspected incident involves a research project, OCRM (ResearchOCRM@ucf.edu) is to be notified along with SIRT.

Failing to comply with federal CUI regulations may result in contractual, financial, and legal penalties to UCF and the individuals(s) involved, including administrative sanctions such as loss of federal funding (directly or indirectly received). Failing to abide by this policy and the related UCF CUI policies, standards, and procedures can result in the suspension of the project until corrective measures are implemented, project termination if deficiencies are not addressed, and disciplinary action up to and including termination of employment and academic expulsion.

DEFINITIONS

Controlled Environment. The systems upon which CUI resides and the physical infrastructure that houses these systems. Examples are the data center housing the servers supporting Knight Shield, or an individual research lab consisting of a room with desktop computers housing CUI, or an office that contains a locked cabinet with CUI materials.

Controlled Unclassified Information (CUI). A category of unclassified federal data defined as information the government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Such information includes controlled technical information, export controlled technical information, financial, business, judicial and all other privileged information like formulas, designs, test results, and other research information that is not in the public domain or cannot be made publicly available when under a federal agreement requiring protection. The [CUI Registry](#), administered by the U.S. National Archives and Records Administration, categorizes and defines the types of information considered CUI, the basis for protections, required markings, and any additional handling instructions.

Data. Alphanumeric or other information represented either in a physical form or digital form suitable for electronic processing or storage.

Data Custodians. Individuals or groups that are considered owners of a particular set of data that may have special or elevated requirements for their protection. Data Custodians are especially important when their data has contractual requirements mandated by a third party, such as data breach notification requirements. Examples of Data Custodians include Principal Investigators (PI's) or units that share UCF data with partner universities.

Highly Restricted Data. A subclassification of Restricted Data, as defined in UCF policy 4-008, *Data Classification and Protection* policy, found on the UCF policy website. Any confidential or personal data that are protected by law or policy, to include protected federal data such as CUI, that require the highest level of access control and security protection, both in storage and in transit.

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems may include electronic media, non-electronic media, and physical environments.

NIST Security Controls. The National Institute of Standards and Technology (NIST) establishes standards and frameworks to guide secure implementations for systems and technology. Federal Regulations ([32 CFR Part 2002](#)) outline the NIST standards to safeguard CUI. NIST Special Publication (SP) 800-171 is required for non-federal information systems. Should UCF *operate* a federal information system on behalf of a federal agency, the Federal Information Systems Modernization Act of 2014 (FISMA) and NIST SP 800-53 apply.

Research Project System Security Plan (RP-SSP). Federal CUI compliance requires a System Security Plan (SSP) to document how security controls are implemented. When operating within Knight Shield, much of this documentation is inherited by a project. The RP-SSP captures the security measures unique to a UCF research project and complements the SSP for the secure enclave housing CUI. The PI completes the RP-SSP template and updates it when changes occur to the members of the research team, external collaborators, IT resources used (hardware and software for specialized instrumentation), external connections required, and the physical office/laboratory security protocols where CUI is generated, stored, and accessed.

Security Event. Any suspicious act that potentially violates federal or state laws, regulations or contracts, or UCF information security policies and computer security standards.

Security Incident. Any act or attempted act that if completed would violate federal or state laws, regulations or contracts, or UCF information security policies and computer security standards. Examples of security incidents include, unauthorized attempts (either failed or successful) to gain access to a computing resource, system, or data; unwanted disruption or denial of service; unauthorized use of an electronic information resource or system for processing or storing data; inappropriate usage according to Policy 4-002, *Use of Information Technologies and Resources*; or the theft or loss of university restricted data (Personally Identifiable Information) as defined by policy 4-008, *Data Classification and Protection Policy*.

SIRT. The Security Incident Response Team (SIRT) is the response team for all information security related events at the University of Central Florida. SIRT will establish protocols to adequately respond, handle, and make appropriate recommendations on the reporting of those incidents within the University's purview. SIRT provides guidance on information and computer security incidents that impact University IT resources or threaten the confidentiality, integrity, and availability of university information.

Sponsored Research. All organized research and development activities sponsored by federal and non-federal agencies and organizations, including university sponsored research that are accounted for and separately budgeted.

Technology. Specific information necessary for the development, production, or use of hardware or software, such as models, engineering designs, blueprints, drawings, technical assistance, or other types of information whether tangible or intangible.

Unauthorized Access. Any action or attempt to utilize, alter, or degrade an electronic information resource in a manner inconsistent with university policies and procedures.

PROCEDURES

The OCRM works hand in hand with the Information Security Office, Office of International Collaboration and Export Control (OICEC), Research Compliance, Network Services, and IT

across the university to achieve the entire realm of compliance for sponsored programs involving CUI.

OCRM assists research teams in navigating compliance requirements by understanding federal regulations, laws, and government policies and providing an infrastructure of people, processes, and technology. OCRM will assist academic, research, and business units and direct support organizations to comply with cybersecurity regulations on non-sponsored activities on a case-by-case basis.

The following sections summarize the procedures to achieve CUI compliance. Refer to the OCRM website at <http://ocrm.research.ucf.edu> for all policies, standards and procedures governing the systems and processes to safeguard CUI.

Planning and Budget

Principal Investigators, research team members, and administrative personnel will assist OCRM with identifying planned research activities involving CUI and determining applicable project-specific security measures to be implemented. Because every research project is unique, *pre-planning is critical*. Sufficient time and budget must be considered upfront, generally in advance of an award, to ensure all technology costs to conduct the research and meet compliance are included in the proposal budget or planned for through some other arrangement.

Ancillary Review Process

OCRM will conduct ancillary reviews and track all proposals and awards identified with cybersecurity requirements to safeguard CUI. Where there is ambiguity or conflicting terms, OCRM will assist the Sponsored Programs Office with the negotiation of terms.

Award Authorization

CUI security controls are to be implemented before the award commences. OCRM will authorize execution of an award involving CUI when the RP-SSP is completed by the PI, and the research team and associated systems handling CUI have been provisioned within an approved environment for CUI. Should extenuating circumstances unduly delay provisioning prior to award, OCRM will authorize execution of the award only upon written assurance by the PI that all required CUI safeguards will be implemented *before* the project receives or generates CUI.

Receiving, Generating, or Safeguarding CUI for Research

Before receiving, accessing, handling, analyzing, or generating CUI, all UCF research team members must execute a standard document known as the RP-SSP acknowledging their understanding of the controlled nature of the information (received or generated) for the sponsored project and the required safeguards with which they must comply.

To ensure awareness of CUI requirements, all personnel responsible for safeguarding CUI, whether on a sponsored agreement or not, will review and acknowledge the Knight Shield User Agreement. The User Agreement is a requirement for Knight Shield account authorization.

Approved Environment

OCRM will support the PI and research team throughout the compliance process and provisioning of IT resources into Knight Shield. Alternative CUI environments require separate planning, funding, and written approval by OCRM in coordination with the CISO. Sponsored research that encompasses UCF operating a federal information system under FISMA will generally operate within Knight Shield; however, due to the separate accreditation process to achieve Authority to Operate (ATO), the exact environment must be determined in coordination with the Office of Cyber Risk Management, Information Security Office, Principal Investigator, and the specific federal agency based on research and operational requirements.

Authorized Systems

Not all university systems may be configured or required to meet CUI compliance. Researchers handling CUI must operate within the approved environment documented in the RP-SSP throughout the period of performance and decommissioning process for the project.

Only systems and removable media devices authorized in writing by OCRM to store, process, or transmit CUI related to a sponsored research agreement may be used.

CUI may not be uploaded to, stored in, or processed by any personal system/device or university system/device not authorized by OCRM. If the system is not on OCRM's list of authorized systems (see website) or documented in an approved RP-SSP, it may not be used. As an example, a deliverable that normally would be uploaded to the UCF Award Tracking System, may not be uploaded if the deliverable contains CUI and the system is not authorized. As an alternative, the PI should upload a PDF of the cover letter (not containing CUI) or other such document reflecting submission instead of the deliverable containing CUI.

Monitoring and Compliance

OCRM is designated with the responsibility to attain and ensure compliance for CUI in accordance with federal regulations and contractual terms of sponsored agreements. UCF CUI environments are also subject to external audit. Periodic assessments may be conducted at any time by internal (UCF) and external (Federal or third-party) risk assessors to affirm compliance. Any deficiencies identified will be documented and shared to the PI. Corrective measures must be implemented by the PI in a timely fashion or compensating controls, approved by OCRM, must be established until such time a full solution can be funded, configured, or otherwise deployed. The university official(s) have the authority to suspend or terminate a research agreement. Further actions may be taken according to the nature, severity, and scope of the deficiencies not addressed or offense identified.

Export Control

For research projects with export control technology, including Controlled Technical Information, per UCF Policy, 4-209, *Export Control Policy*, OICEC is the designated authority charged with compliance oversight of U.S. export control requirements for UCF. OICEC will

determine the export control status and the need for licenses or other authorizations. OCRM will work closely with OICEC to ensure proper security and risk management procedures are in place to meet the CUI safeguarding requirements of the sponsored agreement.

Instructional Steps During the Research Life Cycle

When a sponsored proposal or award involves the protection of CUI, the PI, their information technology contact, research administrator, and research team members will work with OCRM as follows:

At time of Proposal:

1. The PI and their pre-award administrator, in coordination with OCRM, will determine if the sponsored project will receive, possess, and/or create CUI or is otherwise required to implement security controls from the FAR, DFARS 252.204-70xx, NIST SP 800-171, NIST SP 800-172, NIST SP 800-53, or other agency-specific regulation. The applicable question/checkbox on the UCF Proposal Submission Form will be marked for tracking and routing purposes.
2. The PI and their project IT contact, in coordination with OCRM, will determine the information technology resources and solutions required to conduct the research and meet compliance within the authorized controlled environment. Appropriate system solutions may include cost estimates for:
 - a. Communication requirements
 - b. Data Storage and Compute (e.g., Virtual Machine or Desktop in secure enclave)
 - c. Hardware requirements (security and software constraints)
 - d. Data Transfer requirements (cloud, encrypted USB, etc.)
 - e. Instrumentation (bringing lab equipment into enclave)
 - f. Physical Security
 - g. Training
 - h. Background Checks
3. The PI, in coordination with their pre-award administrator, will obtain and include any identified information technology computing price quotes based upon input from OCRM, in the sponsored proposal.
4. When the PI coordinates with OCRM in advance or OCRM identifies a new proposal marked in Huron to require security controls to safeguard CUI, OCRM will offer the PI the RP-SSP to complete, if desired, in advance of award.

At time of Award:

1. When OCRM receives a pending award for review with contractual language to safeguard CUI, where a fundamental research exclusion does not apply, the PI will be notified to complete a RP-SSP if one was not previously established.

- a. To qualify as fundamental research, the research award cannot restrict publication or have dissemination restrictions of the research results or participation of foreign nationals.
 - b. OCRM follows the determination made by the OICEC.
2. PI will complete and return the RP-SSP, or Lab-Wide System Security Plan to OCRM, which is required prior to OCRM authorizing the award to commence. OCRM will review and approve the pending award.
3. OCRM will initiate the onboarding process into Knight Shield and establish a kickoff meeting with the PI, research team, and Knight Shield team. Compliance requirements, use of Knight Shield, and confirmation of IT resource needs outlined in the RP-SSP will be discussed. A physical walk through will be scheduled, if not already previously conducted, and subsequent service tickets will be set up to provision the required IT resources.
4. OCRM will coordinate review of background checks and required training with everyone identified by the PI in the RP-SSP permitted to handle CUI for the project. If a background check is not on file, the PI or their department will coordinate with UCF HR Talent Acquisition and cover the associated costs.
5. Personnel handling or safeguarding CUI must have a background check on file with UCF, complete required training, and review and sign the Knight Shield User Agreement before OCRM will authorize a Knight Shield user account. Each researcher must also review and sign the RP-SSP prior to handling *any* CUI for a project.

During the Award:

If the requirement to handle and safeguard CUI becomes known at time of award or during the award where no prior planning for CUI occurred, the PI will follow the steps normally performed at proposal time to coordinate with OCRM and their pre-award administrator and/or SET Financial Business Center for any price quotes required for approval, budget adjustment, or other authorization for IT computing expenses needed by the Sponsored Programs/Contracts Office for award implementation or modification. See sections above.

1. All personnel are to report suspected abuse, misuse, and cyber incidents to SIRT@ucf.edu and inform OCRM at ResearchOCRM@ucf.edu.
2. The PI must inform OCRM immediately of any changes to project personnel or their status that affects access to CUI for the research project.
3. All personnel handling or safeguarding CUI must maintain their Knight Shield user account, complete annual training, ensure the Knight Shield system(s) assigned to them is accessible for patching and maintenance, and comply with the project-specific RP-SSP, Knight Shield User Agreement, and related procedures set forth by OCRM.
4. Personnel handling CUI must only use systems and devices authorized by OCRM to store, process, or transmit CUI.

- a. This includes university systems located on-premises (or remote if authorized) and cloud resources used to produce documents and other technical deliverables containing CUI, collaborate with others, as well as IT systems that deliverables might typically be uploaded to/stored (e.g., Award Tracking System). Every place CUI is located must be authorized to hold CUI.
 - b. Where proof of submission is needed for a deliverable containing CUI, a PDF of the cover letter (that has no CUI) or other such document reflecting submission to the to the sponsor should be used instead. Follow proper procedures for encryption and methods to transmit the CUI deliverable to the sponsor.
5. PI and research team must assist with continuous monitoring engagements conducted by internal (UCF) and external (Federal and/or third-party) risk assessors to affirm the security controls are implemented and followed.

RELATED INFORMATION

[NARA CUI Registry](#)

[UCF Policy 4-002 Use of Information Technologies and Resources](#)

[UCF Policy 4-008 Data Classification and Protection](#)

[UCF Policy 4-209 Export Control Policy](#)

[UCF Security Incident Response Plan](#)

[UCF Office of Cyber Risk Management:](#)

RELATED DOCUMENTS

[Presidential Executive Order 13556](#)

[32 CFR 2002 Controlled Unclassified Information Final Rule](#)

[NIST Special Publication 800-171, Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#)

[NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations](#)

[Federal Information Systems Management Act of 2014 \(FISMA\), Public Law 113-283](#)

[DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting](#)

[DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements](#)

[DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements](#)

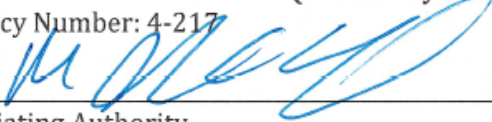



[NASA 1852.204-76 Deviation 21-01, Class Deviation from the NASA FAR Supplement: Implementation of Controlled Unclassified Information \(CUI\) Program](#)

CONTACT

For questions regarding policies and procedures for handling Controlled Unclassified Information please contact the Office of Cyber Risk Management, 12201 Research Parkway, Suite 501, Orlando, Florida 32826-3246, ResearchOCRM@ucf.edu.

INITIATING AUTHORITY

Vice President for Research
Vice President for Information Technology and CIO

POLICY APPROVAL (For use by the Office of the President)	
Policy Number: 4-217	
 _____ Initiating Authority	Date: <u>4/20/23</u>
 _____ Initiating Authority	Date: <u>4/20/23</u>
 _____ University Policies and Procedures Committee Chair	Date: <u>4/13/2023</u>
 _____ President or Designee	Date: <u>5/2/2023</u>