University of CINCINNATI	*Policy Title:* **Controlled Unclassified Information in Research**	*Policy Number:* **1.9.12**
Category: Administration **Policy applicable for:** Faculty/Staff/Students	**Effective Date: 12/14/2023**	**Policy Owner:** VP for Research **Responsible Office(s):** Office of Research Research Security & Ethics Sponsored Research Services

I. Purpose

This research policy outlines requirements for receiving, collecting, developing, handling, storing, processing, and maintaining information that falls into at least one of the Controlled Unclassified Information (CUI) registry categories, as listed on the National Archives and Records Administration (NARA) website. University employees and students who access CUI for research must safeguard this information as outlined by the National Institute of Standards and Technology (NIST) "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" standards (NIST 800-171), NARA, applicable Presidential Executive Orders, and contract clauses. NIST 800-171 defines the requirements for the protection of CUI data to reduce or eliminate inappropriate release of CUI. NARA provides all other pertinent information needed to properly handle CUI. These standards include physical and information technology (IT) security controls including access control, physical security standards, and IT system security.

II. Scope

The following requirements apply to all University of Cincinnati (UC) faculty, staff, and students who receive research funding for, and/or who will have access to information and/or materials/equipment requiring CUI controls.

III. Policy Statement

All proposals (i.e., contract, grant, cooperative agreement, or subaward) that contain or have the potential to involve CUI program components should include appropriate budget line(s) to meet requirements for securing equipment and ensuring compliance. Sponsored Research Services (SRS) shall monitor for CUI requirements in grants and contracts and shall consult with Research Security and Ethics (RSE) to identify UC's responsibilities.

IV. System Security Plan

UC maintains project CUI System Security Plans (SSP) in compliance with federal standards. RSE is responsible for collaborating with Digital Technology Solutions (DTS) and Office of Information Security (OIS) to maintain and update the project SSPs. DTS and OIS are responsible for implementing and maintaining security controls as required by the research contract.

UC Principal Investigators (PI)s who receive funding subject to CUI security requirements shall:

- Complete a NIST assessment with RSE and local IT. NIST assessments must be approved by RSE prior to beginning work on the project and spending funds;
- Solely use University-approved CUI computing services and equipment for all information classified as CUI. Use of standalone computer systems, laptops, tablets, networks or systems not part of the University managed CUI program is prohibited. Use of personally owned equipment/systems for work involving CUI, including but not limited to personally owned laptops, mobile phones and tablets, is prohibited. All devices used must comply with federal regulations regarding prohibited electronic equipment;
- Only perform project-related work in UC-approved areas with physical security controls which meet NIST compliance requirements;
- Store, process, and handle CUI data and materials in environments documented and approved in the project NIST assessment. Storing and handling CUI data and materials in areas not defined and approved in the project NIST assessment is prohibited;
- Email RSE at restricted_research@uc.edu for questions regarding NIST assessment and information technology security requirements for projects with CUI;
- The PI is responsible for immediately reporting any purported violations of the CUI NIST controls to 513-558-ISEC (4732).
- Report potential or real security incidents or breaches to OIS in accordance with the Information Security Incident Management and Response;
- Periodically self-assess the environment and personnel on the project and report any changes or updates to restricted_research@uc.edu; and
- Personally sign and acknowledge the NIST project NIST questionnaire/SSP.

V. Awareness and Training

All UC faculty, staff, and students participating in a CUI project shall complete the appropriate training prior to generating, receiving, or accessing CUI information or project work with CUI regulations. Training requirements outlined in the RSE CUI Guidelines must be completed annually.

VI. Monitoring and Auditing

RSE shall conduct periodic audits of the activities covered by the NIST assessment for each project. Audits may include, but are not limited to, the following:

- Implemented physical security controls;
- Implemented information security controls;
- Personnel review to ensure all researchers are listed in the NIST assessment as participants; and
- Review of training compliance for all participants.

Following the audit, RSE shall review the results with the researchers. If deficiencies are found, the NIST Assessment Team shall work with the PI and DTS to address the deficiencies.

VII. Information Security:

Information system and application logs must be collected and stored for continuous monitoring by OIS. The information logs include, but are not limited to, activities concerning management, resource and system security, and diagnostics. The OIS shall investigate in the case of anomalies or other concerns.

VIII. Exclusions or Special Circumstances

Any exceptions to this policy will be considered on a case-by-case basis. Requests for exceptions must include a justification and should be sent to restricted_research@uc.edu for consideration by RSE, OIS, and the Vice President for Research. A request for exception must receive prior written approval from the Vice President for Research before implementation.

IX. Sanctions

Staff and faculty members who violate this policy could be subject to discipline, up to and including termination, in accordance with applicable University policy, employment agreement, or collective bargaining agreement. Students who violate this policy could be subject to discipline, up to and including dismissal from the University, in accordance with the Student Code of Conduct and/or any applicable code of conduct or policy of their respective college. Moreover, students, staff and faculty members who violate this policy may be subject to other sanctions, including but not limited to, loss of privileges to access UC's approved CUI program, a hold on research funding, or other legal action. Some violations may constitute criminal offenses under local, state, and federal laws.

Additionally, faculty, staff and students could be subject to disciplinary action under the Acceptable Use of Information Technology Policy and the Student Code of Conduct.

References

Cybersecurity Maturity Model Certification (CMMC) framework

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

Executive Order 13556

National Archives Controlled Unclassified Information (CUI) Registry

SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

https://www.uc.edu/content/dam/uc/infosec/docs/policies/Information_Security_Incident_Management_and_Response_Policy_9.1.8.pdf

Related Links

Board rule 10-30-03 – Research: Policy on Sensitive but unclassified research

Board rule 10-30-04 – Policy on Classified Research

Contacts

Office of Research Security and Ethics – Director, Restricted Research – Restricted_research@uc.edu