University of Colorado Colorado Springs

UCCS CAMPUS POLICY

Policy Title: Information Security for Research Compliance

Policy Number: 100-022 **Policy Functional Area:** Administration/Organization

Effective:	December 14, 2023
Approved by:	Jennifer Sobanet, Chancellor
Responsible Vice Chancellor:	Vice Chancellor for Administration and Finance
Office of Primary Responsibility:	Office of the VCAF
Policy Primary Contact:	Chief Information Officer

Reason for Policy: Outlines the baseline expectations for research and information security at UCCS that focus on the compliance protections associated with restricted research, classified research, Controlled Unclassified Information (CUI), and other research security compliance requirements.

I. INTRODUCTION

The purpose of this policy is to provide guidance and outline the baseline expectations for research-related information security at the University of Colorado Colorado Springs (UCCS). A central mission of UCCS is the creation and discovery of knowledge and to openly disseminate that knowledge to the public. This open public process is fundamental to academic freedom, a core and defining principle of the University. UCCS strives to maintain transparent campus environments fully accessible to the university community. While sponsored research is often key to fulfilling the University's mission to create and openly share new knowledge, there are circumstances where conditions of sponsorship potentially impose restrictions. In an increasingly complex research environment, this policy helps to strike a balance between the interests of the agency that requires restrictions and extra protections for research and information and the interests of the University. UCCS expects researchers to be proactive and transparent in their compliance with University, sponsor or agency policies, and state and federal regulations.

II. ROLES AND RESPONSIBILITIES

The policy on Roles and Responsibilities for Sponsored Programs Administration (900-001) contains the primary responsibilities and activities outlined for each defined role. The following are additional responsibilities related only to the requirements for information security for research including

classified research, restricted research, and *Controlled Unclassified Information (CUI)* related research grants and contracts. Calls for proposals, grants, contracts, and other official documents (e.g., a statement of work or MOU) will typically specify if the terms and conditions include research security requirements.

A. Principle Investigator (PI)
    1. Prior to applying for funding that has a relationship with any Government or Corporate agencies that have research security requirements, identify if any CUI *Defense Federal Acquisition Regulation Supplement (DFARs)* clauses are being applied. If a clause is applicable to the award, consult with the Offices of Sponsored Programs and Research Integrity (OSPRI), the Office of Information Technology (OIT), and the Controller's Office to ensure that compliance can be maintained.
    2. The PI will proactively coordinate with OSPRI and OIT to create a *System Security Plan (SSP)* and a *Technology Control Plan (TCP)* (if required) that meet the unique required compliance needs of the project.
    3. The PI is responsible for *awareness and training* for research security and knowing and understanding all clause requirements.
    4. Communicate the details of the SSP with the Department/Grant Administrator and Sponsored Projects Accounting (SPA).

B. Offices of Sponsored Programs and Research Integrity (OSPRI)
    1. Assist PI's with determining if funding being sought requires DFARs clauses, and, if so, determine if the University is able to meet compliance needs of the project. Collect information in the sponsored program submission and award process that assists with this determination.
    2. Review PI's sponsored program budget prior to submission, including determination of the allowability of funding allocated for research security compliance.
    3. If an award is made that includes CUI, OSPRI is available to provide guidance in the PI orientation meeting as well as in the award set-up documentation on specific requirements needed for compliance with the directed federal clauses.
    4. Create and maintain informational resources on the topic of research security and sponsored programs.
C. Office of Information Technology (OIT)
    1. Assist PIs with a consultation prior to submission of a sponsored program proposal that includes CUI to determine if the University is able to remain completely compliant with the outlined requirements.
    2. Consult with the PIs to determine how much to budget, if any, for research security compliance needs in the sponsored program proposal.
    3. When a grant or contract is awarded that contains CUI, OIT is available to provide technical assistance, and guidance on information technology compliance including co-creating a SSP with the PI for the project, performing security assessments, and identifying training opportunities.
    4. Will maintain up-to-date information on the status of research security and resources related to research-security at UCCS.
    5. Be available to assist with monitoring and auditing as outlined in Section III E below.

III. POLICY STATEMENT

A. DISSEMINATION RESTRICTIONS

1. In order to safeguard academic freedom and maintain an open and publicly available campus, UCCS has developed procedures pertaining to the acceptance of outside support that imposes any type of restriction on publication or information dissemination (e.g., publication delays, prohibitions, other restrictions on disclosure, etc). Those operating procedures are maintained by the Offices of Sponsored Programs and Research Integrity.

B. RESTRICTED GRADUATE STUDENT RESEARCH

1. Students must be free to pursue knowledge in an open environment where they are able to access university buildings, university services, and share their research with faculty, students, and the public. Graduate student involvement in *restricted research* projects shall be permitted only when these projects in no way hinder the student's ability to fulfill their degree requirements. Student researchers shall have the opportunity to publish their research findings to obtain degrees and professional recognition.
2. No thesis or dissertation shall be based *exclusively* on a "*restricted research*" project without prior approval from the UCCS Restricted Proprietary and Classified Projects Faculty Committee, nor shall a thesis or dissertation include restricted information that prevents final publication of the degree-required product. Graduate student thesis or dissertation research must adhere to Graduate School and Kraemer Family Library requirements for degree completion.

C. CLASSIFIED ACTIVITIES AND RESEARCH: Some research conducted with or sponsored by the U.S. government is designated as classified. Different levels of classification include top secret, secret, and confidential. At this time, UCCS does not have any facilities (e.g., a Sensitive Compartmented Information Facility, SCIF) to handle classified information. Classified activities and research:

1. Shall only be conducted or discussed on a non-UCCS owned facility with security clearance.
2. Shall only be housed in a cleared facility that is not owned by UCCS.
3. May be part of a researcher's external consulting role if the researcher is cleared for access, the work is carried out in non-university facilities, and is in conformance with the 1/6th rule for outside employment, which must be disclosed via conflict of interest (COI) processes.

D. CONTROLLED UNCLASSIFIED INFORMATION (CUI): CUI is a U.S. Executive Branch data designation that requires safeguarding or dissemination controls. The U.S. Government has responsibility for designating information as CUI. CUI can be collected in many forms, for example as part of human subjects' data collection or research instrument collection. Typically, CUI is identified in the terms and conditions documentation. Such research requires information and information system security controls as identified in law, regulation, or government-wide policy. Common security controls are typically articulated in government contract clauses detailed in Section F. *Cybersecurity Maturity Model Certification (CMMC)* is a method the U.S.

government uses to assess and audit compliance with controls. When information is designated as CUI, the PI is advised as follows:

1. Check the current UCCS CMMC status with the OIT.
2. Include appropriate budget line(s) to underwrite the cost associated with meeting the regulatory, contract, and National Archives and Records Administration (NARA) compliance requirements.
3. If the sponsored program or contract does not include funding, such as unfunded Cooperative Research and Development Agreements (CRADA), researchers should correspond with OIT and OSPRI for a consultation on how to seek and secure necessary components.
4. Complete the appropriate training prior to engaging in research. Training requirements will be outlined in the SSP. Training must be completed annually. Training topics include, but are not limited to, proper handling of CUI and applicable cyber security topics.
5. Researchers who receive federal funding subject to CUI security requirements shall:
    a. Complete a project specific SSP with OIT Security. The University maintains a CUI SSP in compliance with federal standards. UCCS's OIT Security is responsible for maintaining, updating, and controlling the SSP. SSPs are reviewed by the PI and OIT Security. SSPs must be approved by the campus Information Security Officer prior to beginning work on the project and spending funds.
    b. Use University approved CUI computing services and equipment for all information designated as CUI. Use of standalone computer systems or networks or systems not part of the University approved CUI program is prohibited. A standalone computer is separated from a network and generally does not have external connections, including internet.
    c. Store, process, and handle CUI data and materials in environments documented and approved in the SSP. Storing and handling CUI data and materials in areas not defined and approved in the SSP is prohibited.

E. MONITORING AND AUDITING

1. OIT will conduct continuous log monitoring and will audit any CUI funded projects on, at least, an annual basis or more as required or requested. These reviews will cover all applicable security domains specified in NIST 800-171 or outlined in the contract. Reviews may include, but are not limited to, the following:
    a. Implementation of physical security controls.
    b. Implementation of information security controls.
    c. Implementation of any needed TCP for Export Controls or CUI.
    d. Personnel review to ensure all researchers are listed in the TCP/ SSP as participants.
    e. Review of required training compliance for all participants.
2. Conduct a vulnerability assessment of the proposed research environment(s) prior to approving the use of the environment for CUI.
3. UCCS OIT Security will produce a report following their reviews and provide a copy to the PI, OSPRI, SPA, and the PI's supervisor. If deficiencies are found, the OIT Security Group shall work with the PI and unit to address the deficiencies in a timely manner. The specifics of self-assessment activities are outlined in each SSP.
4. The PI is responsible for conducting periodic self-reviews throughout the life of their SSP. OIT is also available to assist with periodic reviews. If there are changes in the project or

individuals participating in the research, the PI must inform OIT Security immediately and these changes will be reflected in the SSP as well. The PI is responsible for informing the campus Information Security Officer of any violations of the SSP immediately upon recognizing the issue.

5. System and Network information logs must be collected and stored for continuous monitoring by OIT. The information logs include, but are not limited to: Logon Activities, *Multi-Factor Authentication, Full Disk Encryption*, Operating System changes, *Anti-Virus* status, File Level Monitoring, and System Level Activities. The activities to be logged are specified in the SSP in accordance with security standards.

F. SECURITY CONTROLS
    1. Any contract or award that contains any DFARS (Defense Federal Acquisition Regulation Supplement) clauses will require different forms of compliance as a function of the specific clause(s). PI's shall ensure compliance with all DFARS clauses and should reach out to the Director of the Office of Research Integrity to build an understanding of the associated requirements and control plans prior to accepting the contract or award.
    2. Research that requires compliance with National Institute of Standards and Technology (NIST) 800-171 clauses are not generally supported by UCCS. Researchers requiring NIST 800-171 may contact OIT on a case-by-case basis to determine feasibility.
    3. Research that requires a Supplier Performance Risk System (SPRS) assessment is generally not supported by UCCS. Researchers require a SPRS assessment of my contact OIT on a case-by-case basis to determine feasibility.

G. ADDITIONAL INFORMATION SECURITY REQUIREMENTS. Additional areas of compliance that may or may not include CUI, but do have guidelines that require compliance with a regulatory body include requirements such as:
    1. Adhere to FAR 52.204-21 Basic Safeguarding of Covered Contractor Information clause which requires additional data security items.
    2. Adhere to NASA Interim Directive 2810-135.
    3. Adhere to Export Control requirements.

H. CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC). CMMC controls will require different forms of compliance. Reach out to OSPRI and OIT prior to a proposal submission to build an understanding of the resources associated with maintaining these compliance requirements.

I. SECURE ACQUISITION OF TECHNOLOGY:
    1. The PI must ensure that any technology purchased for the use of research with research security requirements is purchased from a validated and approved Procurement Service Center vendor. The PI is encouraged to consult with OIT before making any technology purchases to confirm compliance with security controls.

J. ACCOUNTABILITY:
    1. When appropriate, the University will carry out its responsibility to report research security concerns and violations to the appropriate authorities including the funding sponsors, the CU President, law enforcement, and government officials. Concerns and

violations can be reported to any University Official or via the CU Ethics line, which should then be routed to the Chief Information Officer. The CIO may confer with the Chief Security Officer, the Chief Officer of Human Resources, the Provost, the Vice Chancellor for Administration and Finance, the Director for Research Integrity, and Office of University Counsel to determine appropriate actions depending on the scale and scope of the violation.

2. Per APS 1007, serious deviations from accepted practices in proposing, performing, or reviewing research, or in reporting results from research will be subject to UCCS research misconduct procedures.

IV. KEY WORDS

A. *Defense Federal Acquisition Regulation Supplement (DFARS):*
DFARS implements and supplements the FAR. The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public. The DFARS should be read in conjunction with the primary set of rules in the FAR.

B. *Federal Acquisition Regulation (FAR):*
The Federal Acquisition Regulation is the principal set of rules regarding Government procurement in the United States and is codified at Chapter 1 of Title 48 of the Code of Federal Regulations, 48 CFR 1. It covers many of the contracts issued by the US military and NASA, as well as US civilian federal agencies.

C. *Controlled Unclassified Information (CUI)*:
Is a term defined in the Executive Order 13556 as information held by or generated for the Federal Government that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations and government-wide policies that isn't classified under Executive Order 13526 or the Atomic Energy Act, as amended.

D. *Covered Defense Information (CDI)*:
A term defined as unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations and government wide policies.

E. *Cybersecurity Maturity Model Certification (CMMC):*
Is an assessment framework and assessor certification program designed to increase the trust in measures of compliance to a variety of standards published by the National Institute of Standards and Technology (NIST).

F. *National Institute of Standards and Technology (NIST)*
Is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. Its mission is to promote American innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.

G. *System Security Plan (SSP):*
Is a plan of how an information system intends to operate from start up to the end of its life. The purpose of documenting this information is to keep the lifecycle of the system

going from any individual and to allow auditors to easily understand and identify any security problems based on the documentation.

H. *Awareness and Training:*

To bring awareness of a problem to an individual and train them on how to prevent negative actions from happening. In cybersecurity awareness and training helps to ensure that every individual who uses a device understands their responsibilities in protecting the device.

I. *Monitoring and Auditing*:

Monitoring describes the process of detecting cyber threats and data breaches. Which is used during an audit to assess the compliance of the information systems utilized.

J. *Multi-Factor Authentication:*

Electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

K. *Information System:*

A system is a group of interacting or interrelated elements that act according to a set of rules to form a unified whole. A system, surrounded and influenced by its environment, is described by its boundaries, structure and purpose and expressed in its functioning.

L. *Anti-Virus/Malware:*

A computer program used to prevent, detect, and remove malware.

M. *Full Disk Encryption:*

Protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people.

N. *Proprietary Research:*

Sponsored research for which the sponsor or prime contractor requires prepublication review for the purposes of identifying proprietary information or intellectual property to which the sponsor claims ownership.

O. *Restricted Research:*

Relates to agreements that impose restrictions on who can participate in the project, or on the ability of the individual to share information about the project. This may include agreements that: a) restrain the University from disclosing the existence of a contract or grant, the identity of the sponsor or prime contractor, or the purpose and scope of the project; b) require pre-publication review of results beyond 90 days; c) impose limitations on who in the university community may participate in the project (e.g., US citizens only).

P. *Fundamental Research*

Defined by federal regulations as basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

Q. *Classified Research:*

Research that bears a security classification from the federal government, such as top secret, secret, or confidential. Classified research restricts some or all the results, procedures, and personnel working on the project under rules established by the agency for which the research is being conducted.

R. *Sensitive Compartmented Information Facility (SCIF)*

Defined by federal regulations as an area, room, group of rooms, buildings, or installation certified and accredited as meeting Director of National Intelligence security standards for the processing, storage, and/or discussion of sensitive compartmented information.

S. *Technology Control Plan (TCP):*

A TCP is a protocol that outlines the procedures to secure certain export-controlled items (technical data, materials, software, or hardware) are not disclosed to unauthorized personnel or otherwise exported without the necessary U.S. government authorization.

V. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies
   1. APS 6005: Information Security Program
   2. 300-006 Disclosure and Management of Conflicts of Interest or Commitment
   3. 700-002 Responsible Computing
   4. 700-003 Information Technology Security
   5. 900-001 Roles & Responsibilities for Sponsored Programs Administration

B. Procedures
   1. OSPRI Petition to Conduct Restricted and/or Proprietary Projects
   2. Restricted Research: OSPRI Operating Procedures
   3. Research Misconduct Procedures: https://osp.uccs.edu/research-compliance/misconduct-in-research-scholarship-and-creative-activities

C. Guidelines
   1. https://osp.uccs.edu/restricted-proprietary-and-classified-projects
   2. https://oit.uccs.edu/security/ResearchComplianceResources
   3. https://hr.uccs.edu/document-library/conflict-of-interest

D. Other Resources (i.e. training, secondary contact information)
   1. https://oit.uccs.edu/security/export-control
   2. https://rc.uccs.edu/policies
   3. https://compliance.uccs.edu/
   4. CUI Training - https://securityawareness.usalearning.gov/cui/index.html
   5. CUI Categories - https://www.archives.gov/cui/registry/category-list
   6. DFARS 252.204-7000 – Disclosure of Information https://www.acquisition.gov/dfars/252.204-7000-disclosure-information.
   7. DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
   8. DFARS 252.204-7019 – Notice of NIST SP 800-171 DoD Assessment Requirements https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements.
   9. DFARS 252.204-7020 – NIST SP 800-171 DoD Assessment Requirements
   10. https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.

11. DFARS 252.204-7021 – Cybersecurity Maturity Model Certification Requirement
12. https://www.acquisition.gov/dfars/252.204-7021-cybersecuritymaturity-model-certification-requirements.
13. FAR 52.204-21 Basic Safeguarding of Covered Contractor Information https://www.acquisition.gov/far/52.204-21
14. NIST 800-171v2 https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

VI. HISTORY

Initial policy approval	December 13, 2023