

Standards for Handling of Controlled Unclassified Information (CUI)

EXECUTIVE SUMMARY

Duke University School of Medicine (DUSOM) is committed to complying with federal sponsor and contractual requirements to safeguard Controlled Unclassified Information (CUI). These standards outline 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](#). Duke University School of Medicine faculty, 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](#)), National Archives and Records Administration (NARA), applicable Presidential Executive Orders, and contract clauses. All materials classified as controlled unclassified information (CUI) are strictly prohibited by policy from being removed from the Duke Protected Research Compute Cluster (PRCC) environment via any method other than the Honest Broker (HB) with explicit documentation of approval from the Sponsor Agency. Any copy or upload of CUI into systems outside of the PRCC must obtain prior institutional review. Violations of these requirements could result in suspension of PRCC access and appropriate discipline consistent with institutional policies.

DEFINITIONS

Cybersecurity Maturity Model Certification (CMMC): A Department of Defense cybersecurity compliance and assessment program designed to verify that organizations appropriately safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). CMMC requirements are implemented through federal contracts and are based primarily on NIST SP 800-171 security requirements (<https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170>).

Controlled Unclassified Information (CUI): Information that the United States Government creates or possesses, or that an entity creates or possesses on behalf of the Federal Government, that a law, regulation, or government-wide policy requires or permits to be safeguarded or disseminated using specific controls. CUI is not classified information but requires protection from unauthorized access, disclosure, or dissemination in accordance with applicable federal requirements (<https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170>).

System Security Plan (SSP): The authoritative document that describes how a system processes, stores, and transmits Controlled Unclassified Information (CUI), identifies applicable security requirements, and documents the policies, procedures, technologies, and responsibilities used to protect information within the system. The SSP serves as the primary record of the system's compliance with applicable cybersecurity and information security requirements

(https://csrc.nist.gov/glossary/term/system_security_plan).

Duke Protected Research Compute Cluster (PRCC): A Duke Health managed secure research computing environment authorized for the storage, processing, and transmission of Controlled Unclassified Information (CUI) and other sensitive research data in accordance with applicable federal, contractual, and institutional security requirements (<https://medschool.duke.edu/research/research-support/research-support-offices/oasis/school-medicine-research-enclave-sre-2>).

Paper CUI media/labeling: Any hard-copy document or physical medium containing Controlled Unclassified Information (CUI), including printed reports, notes, correspondence, forms, and other paper records. Unless otherwise authorized, paper CUI is prohibited within Duke Health research environment and may not be created, stored, transmitted, or maintained. Users must comply with institutional requirements regarding the identification, handling, and disposition of any authorized paper CUI.

PURPOSE

To protect the research enterprise, establish institutional oversight, and comply with federal laws and regulations pertaining to the management of Controlled Unclassified Information (CUI).

To establish requirements for proper handling of CUI in compliance with CMMC 2.0.

SCOPE

These standards apply to:

- All authorized users (faculty, staff, trainees, authorized affiliates, such as contractors, collaborators, consultants, visiting scholars, and other sponsored external individuals) who have been granted access to Duke resources, such as the PRCC and/or central office support
- All access to the School of Medicine Research Enclave (SRE) Protected Research Compute Cluster (PRCC) for work with CUI
- All systems, networks, and information that include CUI, which must be processed, stored, or transmitted via the PRCC

ROLES AND RESPONSIBILITIES

Each member of the DUSOM community utilizing CUI is responsible for adhering to all federal, state and local laws and Duke University 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. No single individual is permitted to authorize and execute sensitive actions affecting CUI within PRCC.

Principal investigators are expected to ensure compliance with contractual requirements around security, access, and use of CUI; this includes requirements under CMMC and NIST 800-171 standards.

The Technology Steward (Duke OASIS IT team) is responsible for the design, management, and monitoring of the operation of the PRCC.

The Security Steward (Duke Information Security Office (ISO)) is responsible for documenting and testing the security of the system.

The Business Steward (Duke Research Data Support (RDS) team) is responsible for coordinating compliance for users of the system.

STANDARDS STATEMENT

All members of the DUSOM who have a role in receiving, storing, or otherwise processing CUI for research purposes must:

1. Identify and understand their responsibilities when handling CUI, including which elements of the contract have been deemed CUI by the data provider;
2. Comply with contracts with CUI elements, as well as applicable procedures and guidance as described within these standards;
3. Be trained and designated as authorized holders of CUI within the PRCC;
4. Ensure that only authorized individuals are given access to the environment for handling of information containing CUI using a Duke-approved device, unless otherwise specified in the contract;
5. Use the PRCC to receive, store, and process CUI, contingent upon the following:
 - a. paper CUI is not permitted,
 - b. no pictures with mobile devices are permitted, and
 - c. any session that involves working with CUI must be terminated in PRCC once done working with this information;
6. Ensure that all materials classified as controlled unclassified information (CUI) are strictly prohibited by policy from being removed from the PRCC environment via any method other than the Honest Broker (HB) with explicit documentation of approval from the Sponsor Agency;
 - a. Copy or upload of CUI into systems outside of the PRCC is subject to institutional review,

- b. Any material removed from PRCC with approval from the Sponsor Agency must be labelled and safeguarded by the study Principal Investigator in accordance with guidance from the Sponsor Agency.
7. Immediately report Incidents involving CUI to security@duke.edu with information relevant to CUI data handling; and
8. Report non-compliance with these standards to dosi@duke.edu.

TRAINING

All authorized users with access to CUI shall complete the appropriate training prior to generating, receiving, or accessing CUI information or project work with CUI regulations. Training requirements are outlined in the procedural guidance document and must be completed annually with a training roster maintained by the Business Steward.

ENFORCEMENT

Regular audits and monitoring will be conducted to ensure adherence to these standards. Violation of these standards may result in any of the following:

- Revocation of access
- Disciplinary action
- Duke's loss of future contracts containing CUI

CONTACT

For questions related to these standards, please contact dosi@duke.edu.